

Benutzerhandbuch

v1.3

Nomics

NetMonitor

Schöningen, April 2006

2. Auflage 2006

Nomics

Prüssestr. 15

38364 Schöningen

Tel +49 5352/900018

Fax +49 5352/909973

info@nomics.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Inhalt

Dieses Handbuch bietet einen Überblick über die grundsätzliche Bedienung des NetMonitors und soll den Anwender als Unterstützung für den Schnelleinstieg dienen.

In diesem Handbuch werden Ansichten, Menüs und notwendige Einstellungen erläutert.

2 Installation und Inbetriebnahme

Bitte überprüfen Sie nach der Auslieferung den vollständigen Inhalt der gelieferten Komponenten und Unterlagen:

1 * NetMonitor System

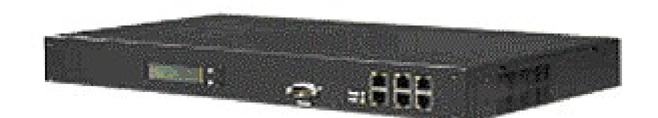


Abbildung 1: NetMonitor

1 * Anschlusskabel für 220 V

1 * Anschlusskabel CAT 5 für Ethernet oder Fast Ethernet

1 * Eckwinkel für die 19” Montage

1 * Benutzerhandbuch

1 * Konfigurationsanleitung für das LCD-Panel

2.1 Montage

Befestigen Sie den NetMonitor mit den 19” Winkeln in einem geeigneten Datenschrank. Bitte achten Sie darauf, dass rechts vom Gehäuse ausreichend kühle Luft zur Verfügung steht, da der NetMonitor die Luft zur inneren Kühlung von der rechten Seite einzieht und nach hinten links ausführt. Bitte achten Sie daher auch darauf, dass hinten links genügend Raum besteht, damit die warme Luft abgeführt werden kann.

2.2 Inbetriebnahmekonfiguration des NetMonitor

Die grundsätzliche Konfiguration des NetMonitor erfolgt über die integrierte webbasierte Bedienoberfläche. Voraussetzung dafür ist die

Erreichbarkeit des NetMonitor im Netzwerk. Vor der Konfiguration ist daher zunächst eine Grundkonfiguration des Netzwerk-Interfaces notwendig.

Die Grundkonfiguration des NetMonitor wird über das integrierte LCD-Panel vorgenommen.

2.2.1 Konfiguration mit dem LCD-Panel

Einstellungen, die über das LCD-Panel vorgenommen werden, gehen bei einem Neustart des NetMonitor verloren. Sie werden nicht permanent gespeichert.

Bitte lesen Sie hierzu die beiliegende Konfigurationsanleitung für das LCD-Panel.

2.2.2 Nach erfolgreicher Grundkonfiguration

Nachrichten im Info-Modus

Alle Nachrichten des Info-Modus werden im Abstand von sechs Sekunden fortlaufend angezeigt. Durch Drücken der Taste _ kann der Info-Modus jederzeit verlassen und damit der Konfigurationsmodus aktiviert werden.

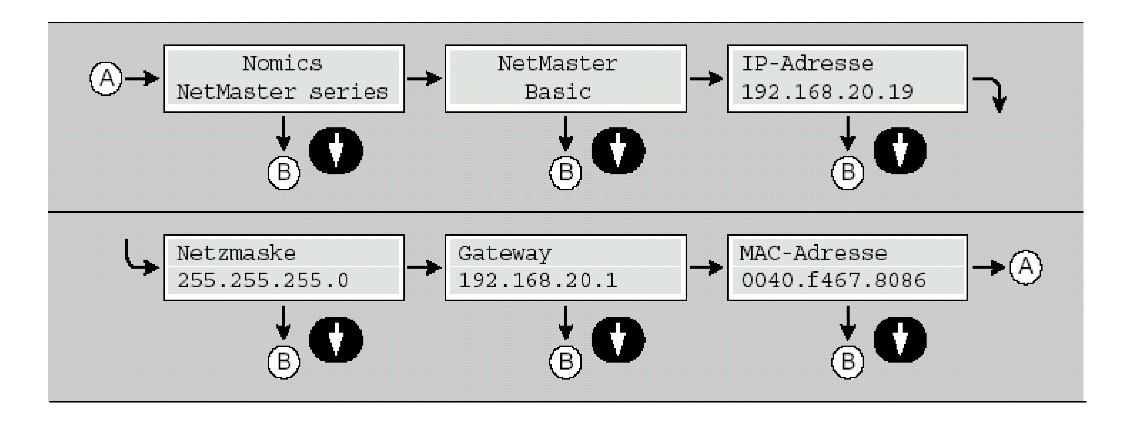


Abbildung 2: Struktur des Info-Modus

Startpunkt ist Label (A). Damit kennzeichnet (A) eindeutig die erste Nachricht im Info-Modus. Nacheinander werden alle sechs Nachrichten angezeigt. Dies geschieht automatisch, daher ist kein Tastensymbol dargestellt. Bei jeder Nachricht kann durch Drücken der Taste _ der Info-Modus verlassen werden. Die Fortsetzung erfolgt bei Label (B).

Ab diesem Punkt sollte der NetMonitor bei erfolgter korrekter Verkabelung, über den Browser zu konfigurieren sein.

Eine weitere Information: Mit NetMaster ist die Basishardware gemeint, sobald die NetMonitor Software geladen wurde, erscheint anstatt des NetMaster NetMonitor.

2.3 Service beim NetMonitor

Falls es notwendig ist, sich an den Service von Nomics zu wenden, befinden sich auf dem NetMonitor alle notwendigen Informationen.

Vorn links beim NetMonitor ist das Nomics Logo zu sehen und an der rechten Seite (von vorn betrachtet) befindet sich die Seriennummer.

Telefon- und Faxrufnummern befinden sich auf dem Deckel (von vorn betrachtet oben links in der Ecke). Ebenso ist dort eine 0700 Zugangsnummer, wie auch eine spezifische E-Mailadresse angegeben.

Die E-Mailadresse und auch die 0700 Zugangsnummer gehören zu der Basis Appliance Nomics NetMaster. Aus Basis des NetMasters ist der Nomics NetMonitor etabliert worden und gehört somit zur Familie der Nomics NetMaster Systeme.

3 Die Anmeldung

Der Zugriff auf das System erfolgt mit Hilfe eines aktuellen HTML-Browsers. Geben Sie in ihren Browser den URL http(s)://192.168.1.140/ ein, wobei Sie hier und im weiteren bitte *192.168.1.140* durch die bei Ihnen gewählte IP Adresse bzw. durch den DNS Namen des **NetMonitor** Systems ersetzen. Sie gelangen zum Anmeldebildschirm.

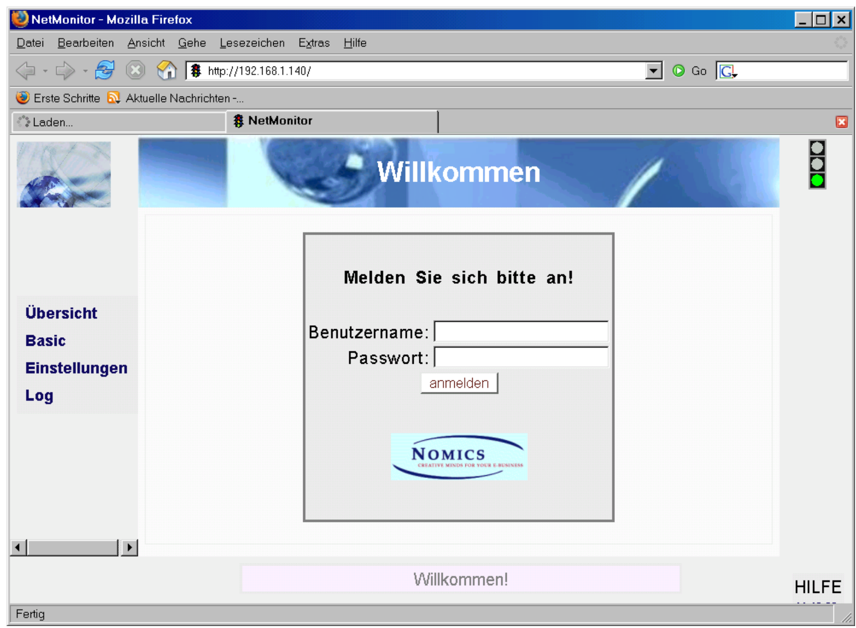


Abbildung 3: Anmeldebildschirm

Im Auslieferungszustand existiert der Benutzername „admin“ mit dem Passwort „Geheim“. Bitte geben Sie die beiden Werte ein und betätigen Sie den Knopf „anmelden“.

Achtung! Groß-/Kleinschreibung wird unterschieden. Der Benutzer „admin“ muss also mit kleinem „a“, das Passwort „Geheim“ mit grossem „G“ geschrieben werden.

4 Übersicht

Nach dem erfolgreichen Anmelden gelangen Sie auf die Übersichtsseite des NetMonitors.

Auf dieser Seite wird der aktuelle Status Ihres Netzerkes angezeigt.

Die Anzeige gliedert sich in drei Teile.

Diese sind die Ampel im Zentrum des Bildschirms sowie links davon die Übersicht über Struktur und Rechts die Übersicht über Funktionen.

Zur Anzeige des aktuellen Status werden die Farben Rot, Gelb und Grün verwendet, welche wie folgt interpretiert werden können.

- Rot = „Kritische Zustand“
- Gelb = „Warnung“
- Grün = „alles OK“

Bei den einzelnen Feldern der Statusanzeigen handelt es sich um Buttons, welche gedrückt werden können. Wenn Sie diese drücken, erhalten Sie Detail-Informationen zu den einzelnen Feldern bzw. den Ursachen der Zustände. Falls mehrere Ursachen bestehen, werden diese untereinander dargestellt.



Abbildung 4: Übersichtsbildschirm

In der unteren Zeile befindet sich die Statuszeile. Hier wird, egal in welchem Bildschirm Sie sich befinden, jeweils der aktuelle Status dargestellt.

5 Basic

Nachfolgend sehen Sie auf der linken Seite das aufgeblendete Basic Menü:

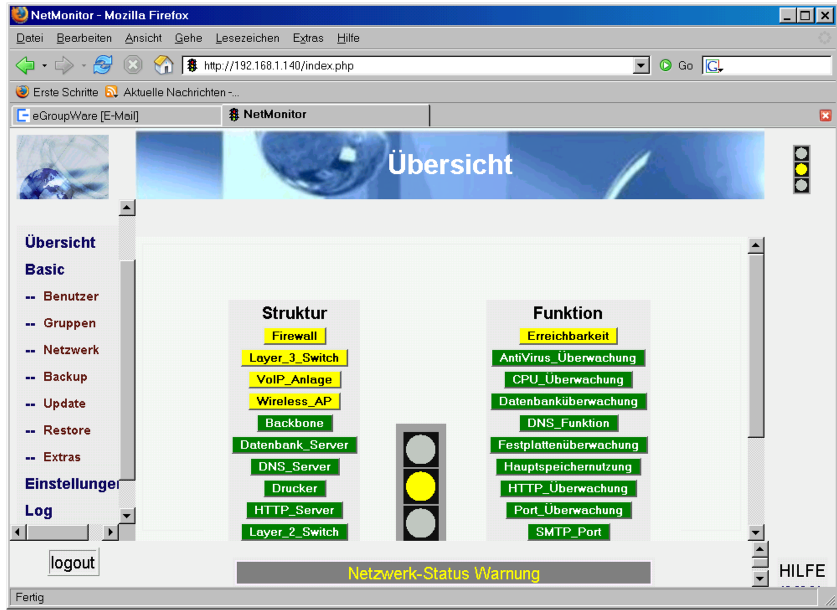


Abbildung 5: Basic Menü

Die folgenden Seiten gehen auf die Basic Konfiguration ein, mit der Sie grundsätzliche Funktionen des System einstellen.

5.1 Rollen/Rechteverwaltung

Beim NetMonitor werden Benutzer und Gruppen unterschieden. Die Bezeichnung Gruppe stellt eigentlich eine Rolle dar. Der Benutzer ist im Sinne eines Anwenders zu verstehen.

5.1.1 Systemauthentisierung und -autorisation

Die Systemauthentisierung- und autorisation ist direkt mit dem Rollen/Rechtemodell verknüpft.

5.1.1.1 Authentisierung

Die Authentisierung beim NetMonitor ist an den Benutzer gebunden. Sie wird durchgeführt indem sich der Benutzer am System über die Loginmaske anmeldet.

5.1.1.2 Autorisierung

Die Autorisation beim NetMonitor ist an den Benutzer gebunden. Die jeweiligen Rechte werden dem Benutzer nach der Authentisierung zugewiesen.

Die erstmalige Zuweisung von Rechten für den jeweiligen Benutzer geschieht bei der Anlage des Benutzeraccounts durch den Administrator.

5.2 Benutzer

Das **NetMonitor** System verfügt über eine einfache Userverwaltung. Im Auslieferungszustand ist der Benutzer „admin“ bereits angelegt. Dieser Benutzer hat Zugriff auf alle Funktionen innerhalb des Systems.

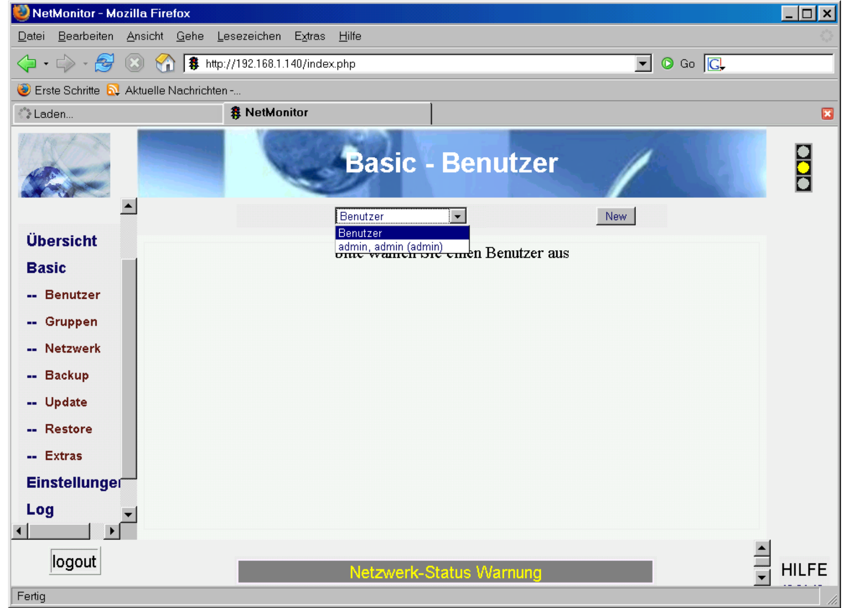


Abbildung 6: Benutzer Menü

Weitere Benutzer können von Ihnen angelegt werden. Diesen Benutzern können Sie Zugriff auf die einzelnen Funktionen des Systems gewähren bzw. verweigern. Dies sehen Sie in Abbildung 7.

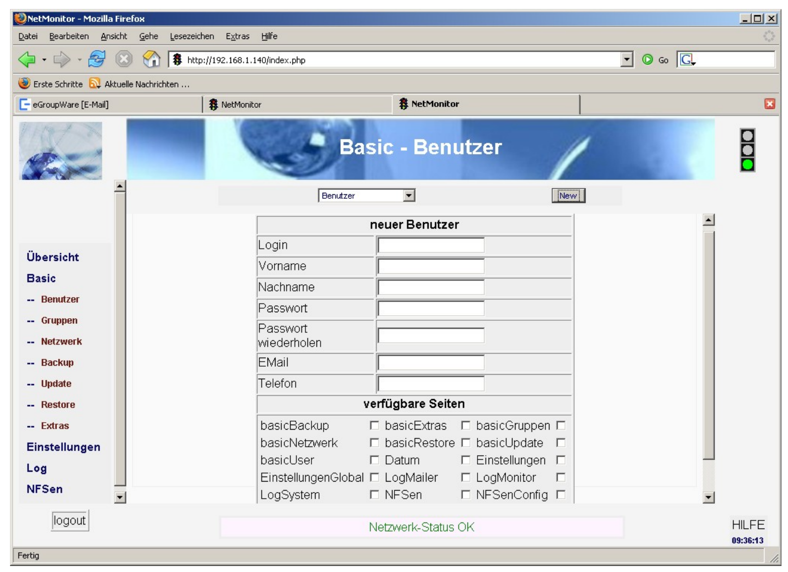


Abbildung 7: Rechteverwaltung beim NetMonitor

5.3 Gruppen

Die Gruppen- oder Rollenfunktionalität wird genutzt um unterschiedlichen Benutzergruppen (daher der Name) im Eventmanagement nutzen zu können. Verschiedene Benutzer sind im NetMonitor eingetragen und haben verschiedenen Verantwortungen. Daher macht es keinen Sinn Fehlermeldungen an alle Benutzer zu versenden, sondern nur an die verantwortlichen Benutzer.

Der NetMonitor nutzt die Gruppen- oder Rollenverwaltung um die EMailbenachrichtigung zu kontrollieren. Hierzu werden Benutzer zu Gruppen zusammengefasst, welche dann bei der Definition von zu überwachenden Objekten zur Benachrichtigung genutzt werden.

Abbildung 8: Gruppen Menü

Das bedeutet EMails werden bei kritischen Zuständen an genau eine Gruppe gesendet.

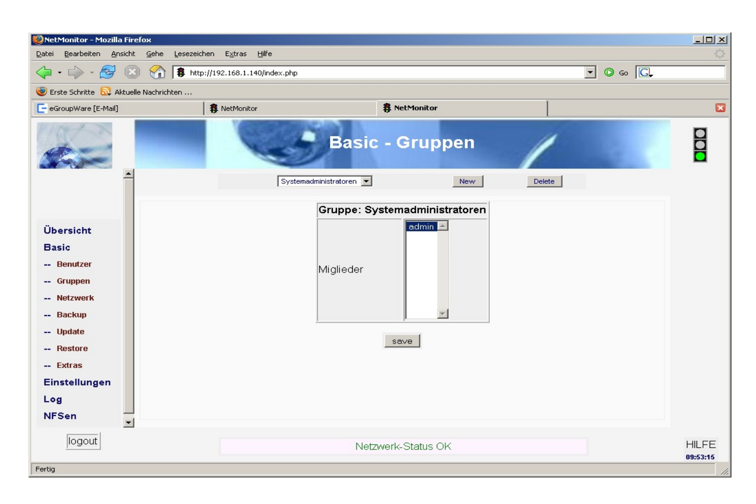


Abbildung 9: Integration von Benutzern in eine Gruppe

In der Abbildung 9 wird der Benutzer “admin” in die Gruppe der “Systemadminstratoren” eingetragen”.

Damit würde der Benutzer “admin” zukünftig Benachrichtigungen aus dem Eventmanagement der Gruppe “Systemadministratoren” an seine E-Mailadresse erhalten.

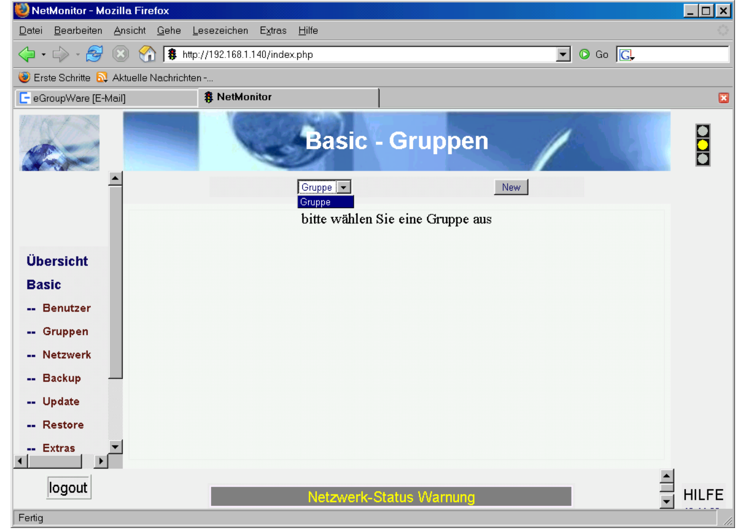
5.4 Netzwerk

Über die HTML-Schnittstelle des **NetMonitor** Systems können Sie folgende Netzwerkeinstellungen vornehmen.

- Hostname
- IP Adresse
- Netzmaske
- Default-Gateway
- Nameserver 1
- Nameserver 2
- EMail Relay Host

Abbildung 10: Netzwerk Menü

Achtung! Durch die Änderung der IP Konfiguration ist das System unter dem alten URL natürlich nicht mehr erreichbar. Sie müssen in Ihren



Browser die neue IP Adresse eingeben und sich neu anmelden.

5.5 Backup

Für die Sicherung des **NetMonitor** Systems stehen Ihnen zwei Methoden zur Verfügung: USB und FTP. Beide Methoden können einmal täglich zu einer von Ihnen bestimmten Uhrzeit durchgeführt werden und beide Methoden können gleichzeitig aktiviert sein.

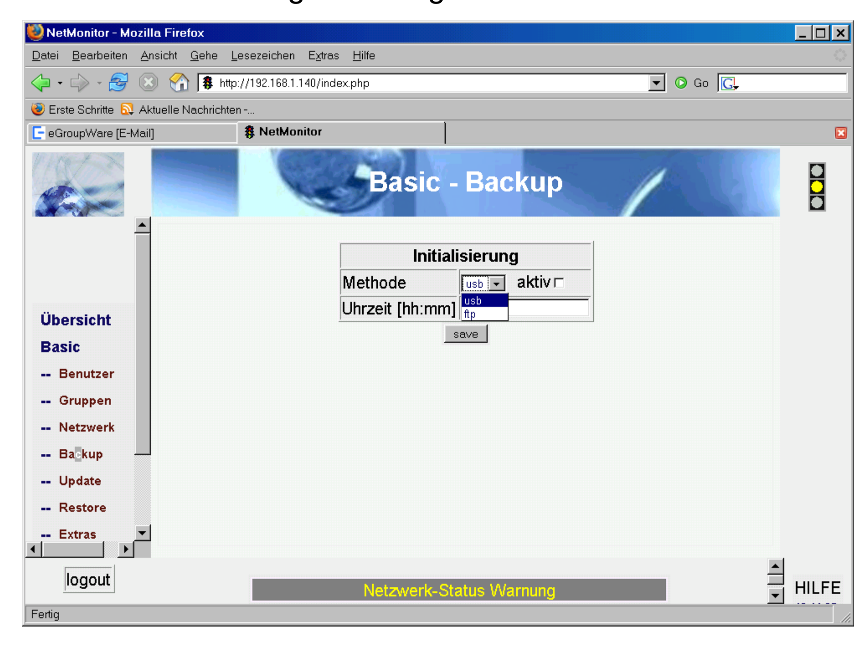


Abbildung 11: Backup Menü

5.5.1 Backups auf einen USB Stick speichern

Auf der Rückseite der **NetMonitor** Systeme kann ein USB Gerät angesteckt werden. Diese USB Schnittstelle ist für den zum Lieferumfang gehörenden USB Stick vorgesehen. Mit Hilfe des USB Sticks können einfach Backups des **NetMonitor** Systems erstellt werden, und im Fehlerfall, können von dort die Daten wieder zurückgespielt werden.

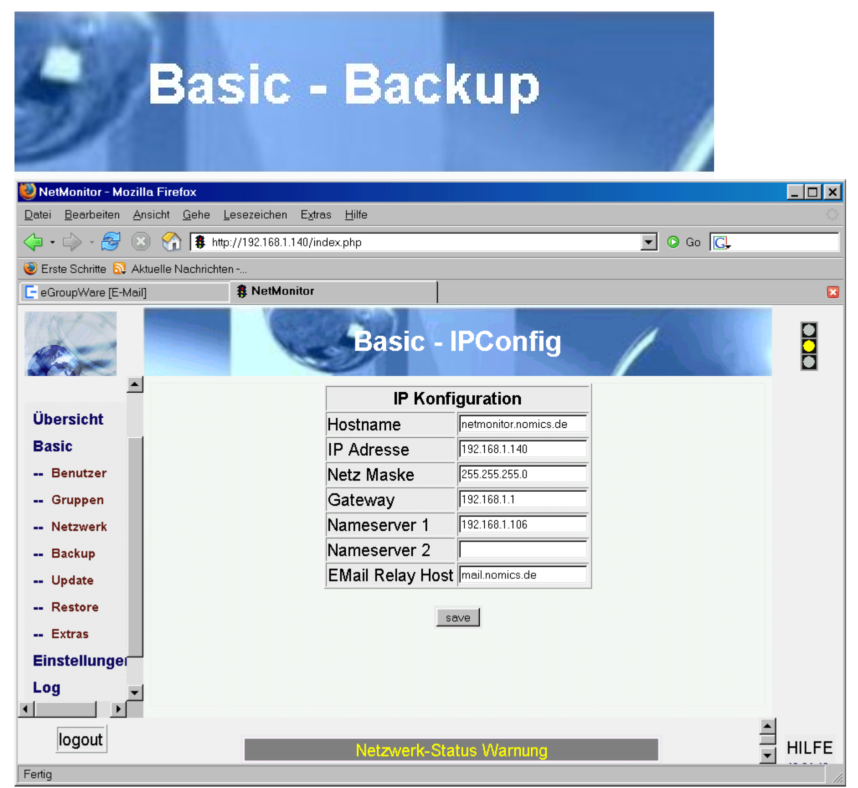


Abbildung 12: Backup Menü, aktivieren

Konfiguration des Backups auf den USB Stick:

- Wählen Sie als Methode „USB“ aus den Popup-Menü aus
- Setzen Sie den Haken bei „aktiv“
- Geben Sie die Uhrzeit an, zu der das Backup durchgeführt werden soll
- Speichern Sie Ihre Eingaben mit dem Knopf „save“

Danach werden jeden Tag zu der von Ihnen angegebenen Uhzeit Backups auf dem USB Stick abgelegt. Dabei wird immer dafür gesorgt, dass für das aktuelle Backup auf dem USB Stick ausreichend Speicherplatz zur Verfügung steht, indem ggf. alte Dateien gelöscht werden.

Achtung! Damit keine Backup-Dateien verloren gehen sorgen Sie dafür, dass der USB Stick tatsächlich im Gerät ist und auch angesprochen werden kann. Bei dem ausgeliefertem Stick erkennen Sie letzeres an der leuchtenden grünen LED.

Achtung! Benötigen Sie einen neuen USB Stick oder möchten Sie einen eigenen verwenden, wenden Sie sich bitte zuvor an den **NetMonitor** Support unter der eMail Adresse netmonitor@support-group.de.

5.5.2 Backups auf einem FTP Server sichern

Als Alternative oder als zusätzliche Sicherungsmassnahme können Sie Backups auch auf einem FTP Server ablegen. Gehen Sie dazu wie folgt vor:

- Wählen Sie aus dem Popup-Menü die Methode FTP aus
- Setzen Sie den Haken bei „aktiv“
- Bestimmen Sie die Uhrzeit, zu der täglich ein Backup auf dem FTP Server abgelegt werden soll
- Geben Sie den Namen eines Users an, der auf dem FTP Server Dateien ablegen darf
- Ist auf dem FTP Server für den User ein Passwort notwendig, geben Sie dieses bitte ein und bestätigen Sie es bei „Passwort wiederholen“
- Geben Sie die IP Adresse des FTP Servers ein
- Und bestimmen Sie das Verzeichnis auf dem FTP Server, in das die Backup-Dateien abgelegt werden soll

Nachdem Sie die Daten mit dem Knopf „save“ in die Datenbank übernommen haben, wird das Backup jeden Tag zu der von Ihnen angegebenen Uhrzeit auf dem FTP Server abgelegt.

Achtung! Um Datenverlust zu vermeiden, prüfen Sie regelmässig auf dem FTP Server, ob aktuelle Backup-Dateien vorhanden sind. Prüfen Sie auch, ob genügend Speicherplatz auf dem FTP Server zur Verfügung steht.

5.6 Restore

Wenn Sie eine oder am besten beide Backup-Methoden aktiviert haben, sind Sie vor schwerwiegendem Datenverlust geschützt – im Fall der Fälle können Sie mit der Funktion „Restore“ des Service-Moduls Basic die Daten zum Zeitpunkt der letzten Datensicherung wieder herstellen. Sollte die Hardware nicht mehr funktionstüchtig sein, können Sie Ihren Datenbestand auf einem neuen Austausch-System wieder herstellen.



Abbildung 13: Restore Menü

5.6.1 Wiederherstellen der Daten von einem USB Stick

Wählen Sie aus dem Menü des Service-Moduls „Basic“ die Funktion „Restore“.

Wenn ein USB-Stick eingesteckt ist und auf diesem Backups vorliegen, so werden diese in der Tabelle „vorhandene Backups auf USB “ aufgelistet.

Aus dieser Liste können Sie die Datei auswählen, deren Datenbestand Sie wiederherstellen möchten. In den Dateinamen sind das Datum und die Uhrzeit kodiert, zu denen das Backup erstellt worden ist. Betrachten wir als Beispiel den letzten Eintrag in der Liste, „nmb_usb-20040625-1700.tgz“. Es handelt sich...

- um ein **NetMonitor** Backup (nmb),
- das auf dem USB Stick abgelegt worden ist (usb),
- das am 01. April 2006 (20060401),
- um 15:10 Uhr erstellt worden ist (1510).

Rechts neben den Dateinamen ist jeweils ein Knopf „wieder herstellen“ vorhanden. Durch Betätigen eines dieser Knöpfe kann der entsprechende Datenbestand wiederhergestellt werden.

Vor dem tatsächlichen Herstellen müssen Sie den Vorgang nocheinmal bestätigen.

Achtung! Vor einem Restore wird der aktuelle Datenbestand nicht gesichert! Ggf. sollten Sie über die Backup Funktionen eine aktuelle Sicherung erstellen lassen. Setzen Sie hierzu die Backup-Zeit bei der Methode „USB“ oder „FTP“ auf einen nahen Zeitpunkt, z.B. in fünf

Minuten, und führen Sie das Restore erst aus, wenn die Sicherung erstellt worden ist.

5.6.2 Wiederherstellen der Daten von einem FTP Server

Um Daten aus einem Backup wiederherzustellen, das auf einem FTP Server abgelegt worden ist, müssen Sie die Datei zunächst von dem FTP Server auf Ihren lokalen Rechner ablegen. Benutzen Sie hierzu den von Ihnen bevorzugten FTP Client.

Nachdem die Datei lokal auf Ihrem Rechner vorliegt, kann diese mit Hilfe der HTML -Oberfläche auf das **NetMonitor** System übetragen werden. Drücken Sie hierfür den Knopf „Browse“. Es öffnet sich ein Dialog, mit dem Sie die zuvor auf Ihrem Rechner abgelegte Datei auswählen können.

Nachdem Sie „Öffnen“ gedrückt haben, erscheint die Dateiauswahl in dem Textfeld „Restore File“. Drücken Sie nun auf „senden“, wird die Datei von Ihrem lokalen Rechner auf das **NetMonitor** System übertragen.

Anschließend erscheint die übertragene Datei in der Dateiliste „Temporäres Restore-Verzeichnis“ und kann über den Knopf „wieder herstellen“, der rechts neben dem Dateinamen angeordnet ist, eingespielt werden. Vor der tatsächlichen Ausführung müssen Sie den Vorgang mit dem Knopf „OK“ im nächsten Fenster bestätigen.

Achtung! Vor einem Restore wird der aktuelle Datenbestand nicht gesichert! Ggf. sollten Sie über die Backup Funktionen eine aktuelle Sicherung erstellen lassen. Setzen Sie hierzu die Backup-Zeit bei der Methode „USB“ oder „FTP“ auf einen nahen Zeitpunkt, z.B. in fünf Minuten, und führen Sie das Restore erst aus, wenn die Sicherung erstellt worden ist.

5.7 NetMonitor Update

Im Rahmen der Produktpflege und der Fehlerbeseitigung werden in unregelmässigen Abständen Updates des **NetMonitor** Systems zur Verfügung gestellt. Mit der Funktion „Update“ des Service-Moduls Basic können diese eingespielt werden.

Achtung! Die Verfügbarkeit neuer Updates wird über eMails bekannt gegeben. Lassen Sie sich unter der eMail Adresse netmonitor@support-group.de registrieren, um Informationen hierzu zu erhalten.

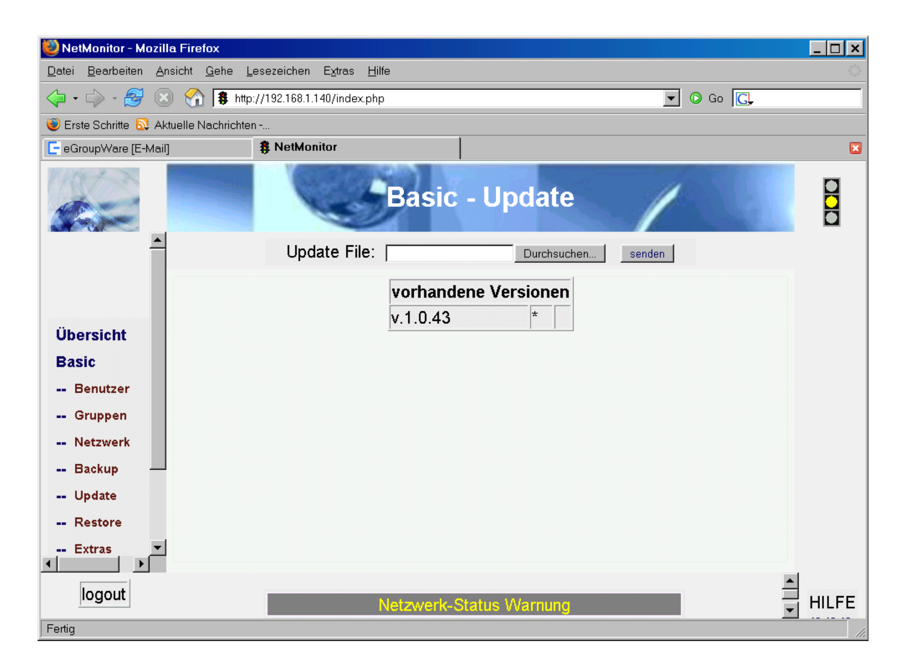


Abbildung 14: Update Menü

Mit der Information, dass Updates vorhanden sind, erhalten Sie auch Angaben dazu, wo Sie diese beziehen können.

Haben Sie eine Update Datei auf Ihrem lokalen Rechner abgelegt, können Sie diese über die Dateiauswahl „Browse“ selektieren und anschließend mit dem Knopf „senden“ auf das **NetMonitor** System übetragen. Dort wird die neue Version automatisch installiert, jedoch noch nicht aktiviert.

In der Liste „vorhandene Versionen“ erhalten Sie einen Überblick der zur Zeit auf dem System vorhandenen Versionen. Mit dem Knopf „aktivieren“ können diese ausgewählt werden.

5.8 Extras

Im MenuPunkt „Extras“ haben Sie die Möglichkeit Informationen wie SNMP-OIDs und Server Ports zu definieren bzw. zu hinterlegen. Diese Informationen sind für die Funktionsweise der Überwachung notwendig. Diese einmalig einzutragenen Informationen stehen Ihnen dann später zu gegebener Zeit als Auswahllisten zur Verfügung. Das hat zum Vorteil, das Sie sich nicht merken müssen, welche SNMP OIDs welche Werte liefern.

Es existieren drei Tabellen, welche folgend aufgelistet und kurz beschrieben sind:

- „Service Ports“
    - definieren Sie hier, welche Ports Sie planen zu überwachen.
    - z.B. Port 80 für HTTP
        - Beschreibung: **HTTP**
        - Wert: **80**

- „SNMP Description“
  - ➢ wird genutzt um Objekte eine Beschreibung zu geben.
  - ➢ gibt z.B. bei Interfaces deren Namen an
- „SNMP UIDs“
  - ➢ Die UID des Wertes, welchen Sie mit SNMP abfragen möchten.

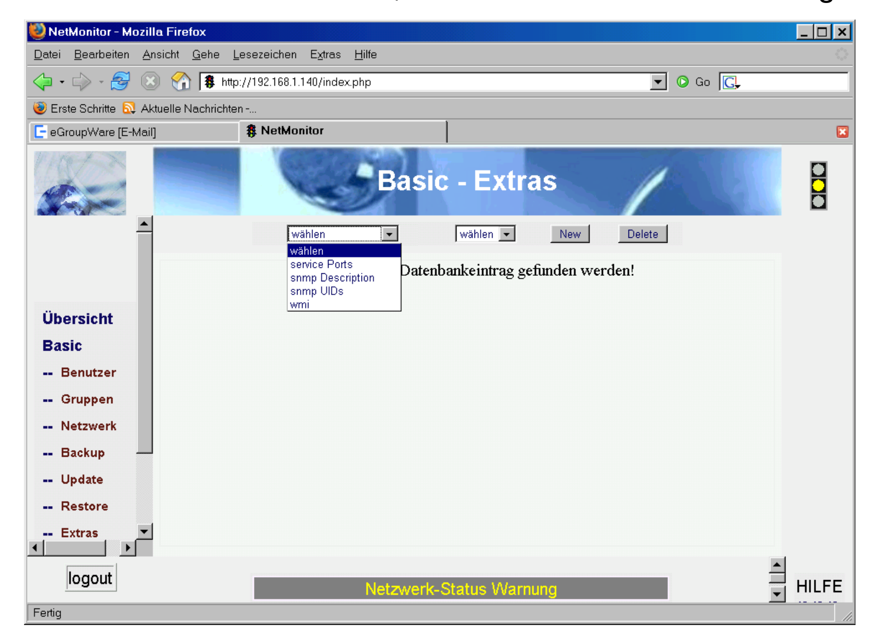


Abbildung 15: Extras Menü

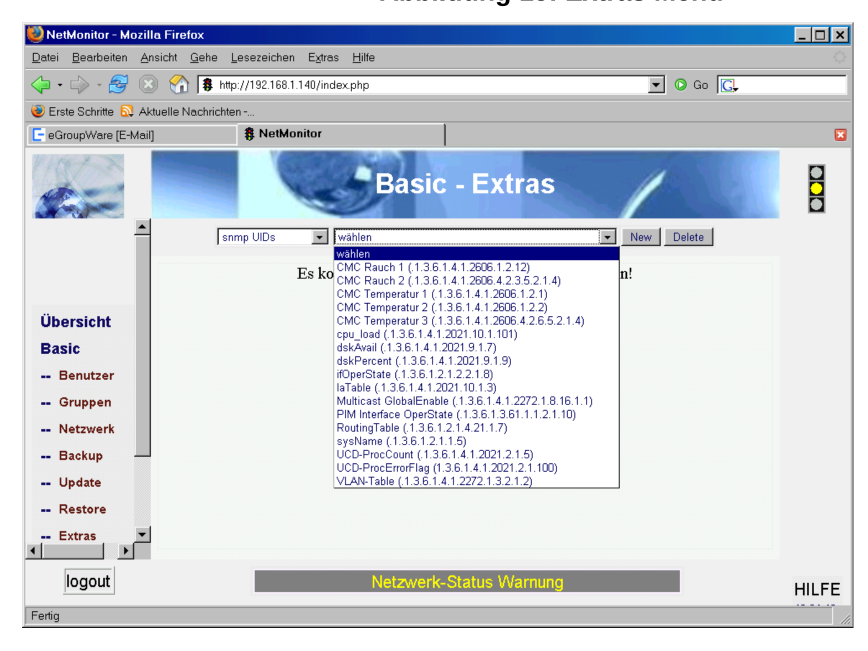


Abbildung 16: Extras Menü –SNMP UIDs

Die SNMP UIDs können frei eingestellt werden. Die wichtigsten werden beim NetMonitor bereits mitgeliefert.

6 Einstellungen

Im Punkt Einstellungen werden alle die Überwachung betreffenden Konfigurationen vorgenommen.

Hier wird unterschieden zwischen

- „Global“
- „Systems“
- „und alles andere“



Abbildung 17: Menü Einstellungen

Solange der NetMonitor noch nicht weiter konfiguriert ist, werden Sie nur die beiden Menüpunkte “Global” und “Systems” vorfinden. Alle weiteren Menüpunkte entstehen während der Konfiguration.

Ebenso entstehen quasi während der Konfiguration die Einträge in dem Übersichtsbildschirm.

6.1 Kurzer Funktionsüberblick

Der NetMonitor basiert auf der Grundüberlegung, das eine einzelne Information zu wenig Inhalt bietet um sicher, schnell und effizient in eine eventuell notwendige Feherbehandlung einzusteigen.

Normalerweise wird der NetMonitor für die Früherkennung von künftigen Fehlersituationen eingesetzt. Treten während des Monitorings der Objekte Fehler oder Probleme auf, so werden sie sofort mit entsprechendem Informationsgehalt an die zuständigen Personen gemeldet.

Möglich wird dies durch die Art der Überwachung. Beim NetMonitor wurde das grundsätzliche Prinzip eines “Fadenkreuzes” umgesetzt.



Fadenkreuz zur Überwachung

Über das Monitoring von zwei unterschiedlichen Funktionsinhalten (dargestellt als X-Ache und als Y-Achse), kann man sehr genau auf die mögliche Störungen reagieren.

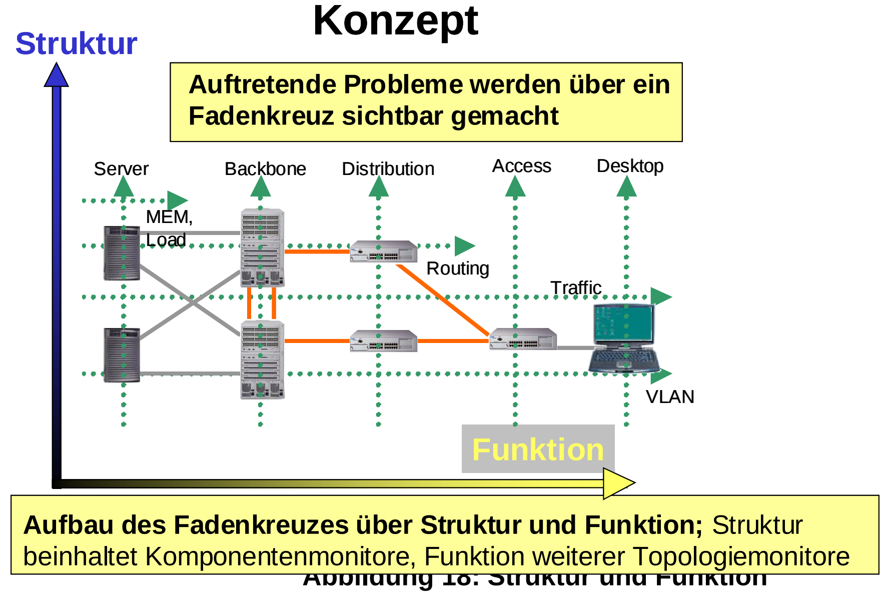


Abbildung 18: Struktur und Funktion

Die Y-Achse wird beim NetMonitor als Struktur dargestellt und die X-Achse wird als Funktion dargestellt.

Im obigen Konzept sehen Sie Server, Backbone, Distributionsbereich, Accessbereich und der Desktop als Struktur dargestellt. In der Funktion sehen Sie Memory, CPU Load, Routing, Traffic und VLAN dargestellt.

Im NetMonitor werden die einzelnen Monitore jeweils der Kategorie Struktur oder der Kategorie Funktion zugeordnet. So erhält man ein „Fadenkreuz“, welches man sich selbst zusammen stellen, bzw. konfigurieren kann.

Zuerst muss das zu überwachende System konfiguriert werden, danach werden jeweils die notwendigen Monitore für dieses System konfiguriert.

6.2 Systems

Bevor Sie beispielsweise auf einem System den Verbrauch der Festplatte oder den Status des MailServer überwachen können, müssen Sie das System eintragen.

Wählen Sie hierzu den MenuPunkt „Systems“, drücken den Button „new“, füllen die Felder aus und vergessen Sie nicht zu speichern durch drücken von „save“.

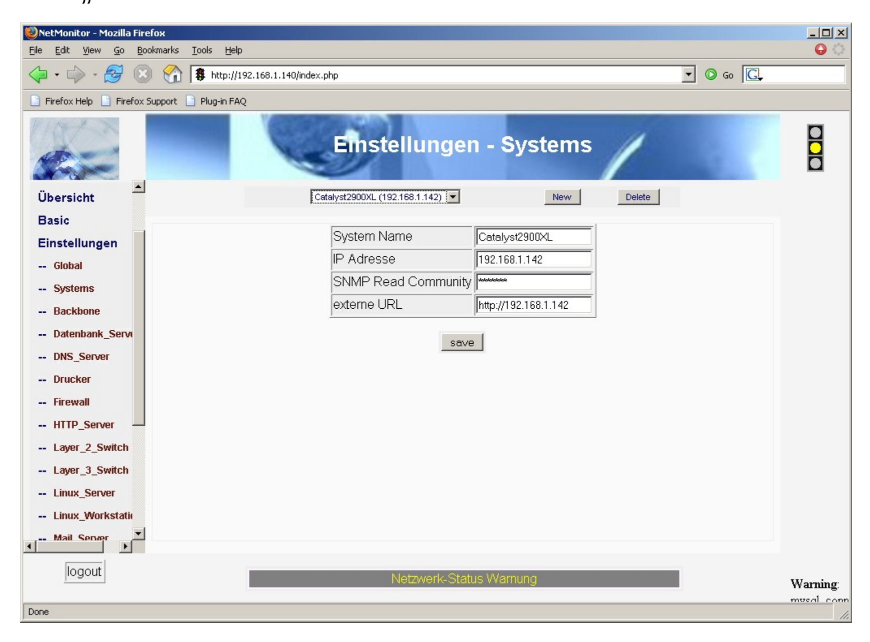


Abbildung 19: Konfiguration eines Systems

Folgende Werte für Systeme können eingetragen werden:

- System Name

  ein beliebiger Name, welcher als Beschreibung des Systems gilt

- IP Adresse

  gültige IP-Adresse des Systems

- SNMP Read Community

  gültige SNMP Read Community

- externe URL

  hier können Sie beispielsweise die URL zur Konfiguration des Systems hinterlegen um im Problemfall direkt dorthin zugelangen.

6.3 Global

An dieser Stelle wird die Definition aller zu überwachenden Objekte vorgenommen, also die Konfiguration der einzelnen Monitore.

Alle existierenden Objekte werden in einer Tabelle aufgelistet.

Durch klick auf ein Objekt kann dieses geändert oder gelöscht werden.

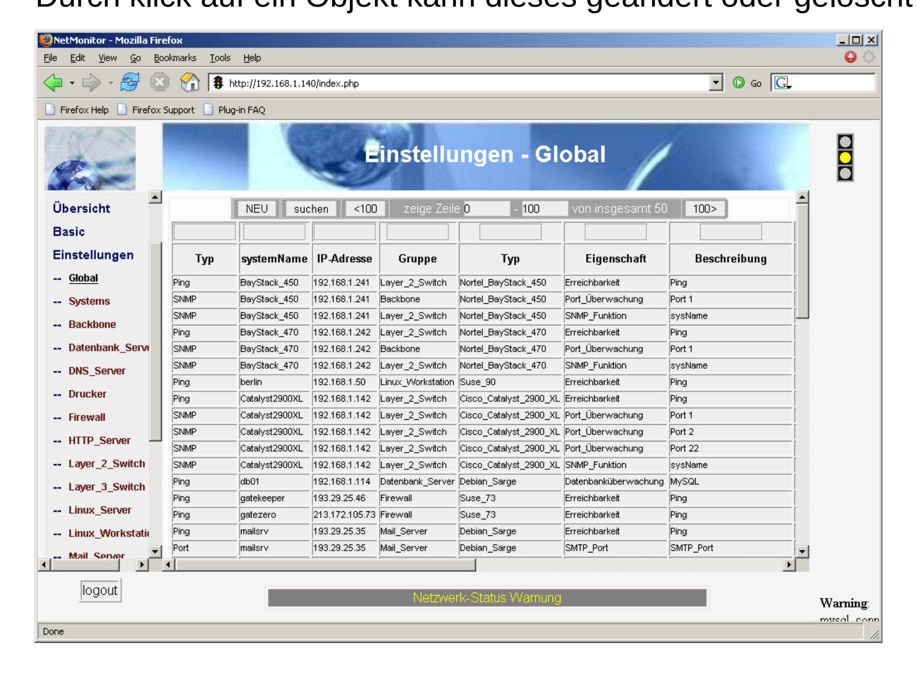


Abbildung 20: Konfiguration der einzelnen Monitore

Um ein neues Objekt anzulegen drücken sie „NEU“. Wählen Sie im sich öffnenden Fenster „um welchen ÜberwachungsTyp, bzw Methode der Überwachung“ es sich handelt:

- Port

  Prüft einen angegeben Port auf Aktivität

  z.B. „Ist Port 80 auf WebServer aktiv“

- Prozesse

  Prüft ob ein Prozess auf einem WinowsSystem läuft.

  z.B.: „Läuft MSSQL auf Server MEINWINDOWSDBSERVER“

- SNMP

  nutzt anzugebene SNMP-OIDs

Wenn Sie eines der Typen gewählt haben, öffnet sich ein neues Formular, in dem Sie die Definition eines Objektes vornehmen können.

In diesem Formular werden Sie auch die unter „Basic – Extras“ eingetragenen Informationen wiederfinden.

Im Formular zum Typ SNMP steht ein Button „Initialisieren“ zur Verfügung.

Wenn Sie diesen Button drücken, wird versucht für die eingetragen Werte Informationen vom System zu lesen.

Hierfür wird „snmpBeschreibung“ genutzt.Wollen Sie z.b. 48 Ports auf einem Switch überwachen, so tragen Sie den ersten Ports ein, speichern diesen und drücken Initilisieren. Als Ergebnis werden alle auf dem Switch vorhanden Ports unter verwendung ihrer Portbeschreibung als Objekte im NetMonitor eingetragen.

6.3.1 Navigation in Global

Im Menue “Global” ist eine effiziente Navigation etabliert worden. In kleinen Netzwerken reichen möglicherweise 50 – 70 Monitore aus um alles wichtige zu überwachen. In mittleren Netzwerken ist man schnell bei 200 – 300 Monitoren und mehr.

Da physikalisch auf einem Bildschirm nur eine gewisse Menge an Informationen unterzubringen ist, werden automatisch die angezeigten Monitore nach einer von Ihnen einstellbaren Menge auf eine neue Bildschirmseite umgebrochen.

6.3.1.1 Listen in Global

Per default sind beim NetMonitor 100 Monitore zu sehen. Sie können dies änderbn, indem Sie in der Navigation bei”zeige” einen anderen Wert einstellen.



Abbildung 21: Navigation in Global

Die Logik der Navigation unterstützt Sie bei der Suche von speziellen Monitoren. So können Sie in der Navigation einstellen, das Sie die Monitore von 450 – 500 sehen wollen, indem Sie bei “zeige” 50 eingeben und bei “ab Zeile“ 450 eingeben. Mit “Klick” auf “suchen” werden Ihnen die gesuchten Monitore in einer Liste auf dem Bildschirm dargestellt.

6.3.1.2 Suchen in Global

Ebenso, wie die Listenerstellung, besteht eine effiziente Suche in Global.



Einstellungen - Global

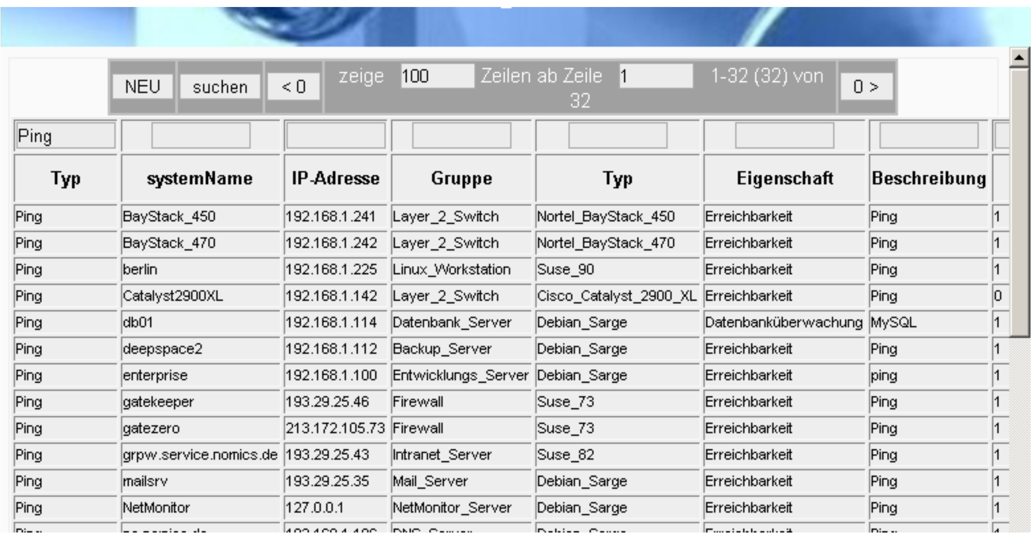
NEU | suchen | < 0 | zeige 100 Zeilen ab Zeile 1 | 1-100 (100) von 513 | 100 >

Typ	systemName	IP-Adresse	Gruppe	Typ	Eigenschaft	Beschreibung	IstWert
Ping	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Erreichbarkeit	Ping	1
SNMP	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Forwarding_DataBase	BayStack_FDB	-1
SNMP	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Interface_Discards	Interface_in_discards0	0
SNMP	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Interface_Discards	Interface_in_discards0	0
SNMP	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Interface_Discards	Interface_in_discards0	0

Abbildung 22: Suchen im Global

Hierzu werden die freien Felder unterhalb der Listenfelder oder oberhalb der Monitorbeschreibungen genutzt.

Wenn man z.B. einen bestimmten Monitor sucht (ping auf mailsrv), so gibt man links beim Monitortyp den ersten Suchbegriff ein. Hier ist es“ping“. Mit Klick auf „suchen“ haben sie eine Liste aller entsprechenden Monitore.



NEU | suchen | < 0 | zeige 100 Zeilen ab Zeile 1 | 1-32 (32) von 32 | 0 >

Ping

Typ	systemName	IP-Adresse	Gruppe	Typ	Eigenschaft	Beschreibung	
Ping	BayStack_450	192.168.1.241	Layer_2_Switch	Nortel_BayStack_450	Erreichbarkeit	Ping	1
Ping	BayStack_470	192.168.1.242	Layer_2_Switch	Nortel_BayStack_470	Erreichbarkeit	Ping	1
Ping	berlin	192.168.1.225	Linux_Workstation	Suse_90	Erreichbarkeit	Ping	1
Ping	Catalyst2900XL	192.168.1.142	Layer_2_Switch	Cisco_Catalyst_2900_XL	Erreichbarkeit	Ping	0
Ping	db01	192.168.1.114	Datenbank_Server	Debian_Sarge	Datenbanküberwachung	MySQL	1
Ping	deepspace2	192.168.1.112	Backup_Server	Debian_Sarge	Erreichbarkeit	Ping	1
Ping	enterprise	192.168.1.100	Entwicklungs_Server	Debian_Sarge	Erreichbarkeit	ping	1
Ping	gatekeeper	193.29.25.46	Firewall	Suse_73	Erreichbarkeit	Ping	1
Ping	gatezero	213.172.105.73	Firewall	Suse_73	Erreichbarkeit	Ping	1
Ping	grpw.service.nomics.de	193.29.25.43	Intranet_Server	Suse_82	Erreichbarkeit	Ping	1
Ping	mailsrv	193.29.25.35	Mail_Server	Debian_Sarge	Erreichbarkeit	Ping	1
Ping	NetMonitor	127.0.0.1	NetMonitor_Server	Debian_Sarge	Erreichbarkeit	Ping	1

Abbildung 23: Suche über Typ

Falls der gesuchte Monitor noch nicht dabei ist, können Sie die Suche weiter spezifizieren.

Der nächste Eintrag wäre in unserem Beispiel „mailsrv“ im Feld „systemname“. Mit klick auf „suchen“ sehen Sie eine Liste aller Monitore in denen beide Begriffe vorkommen.



NEU | suchen | < 0 | zeige 100 Zeilen ab Zeile 1 | 1-1 (1) von 1 | 0 >

Ping | mailsrv

Typ	systemName	IP-Adresse	Gruppe	Typ	Eigenschaft	Beschreibung	IstWert	Vergleich
Ping	mailsrv	193.29.25.35	Mail_Server	Debian_Sarge	Erreichbarkeit	Ping	1	==

Abbildung 24: Suche mit mehreren Optionen

In unserem Beispiel haben wir den gesuchten Monitor gefunden.

6.4 Konfiguration der Überwachungsmethoden

Im Menü “Global” stehen zur Konfiguration der einzelnen Monitore spezielle Methoden zur Verfügung. Diese stellen die Grundüberwachungstechnologie für einen Monitor zur Verfügung.

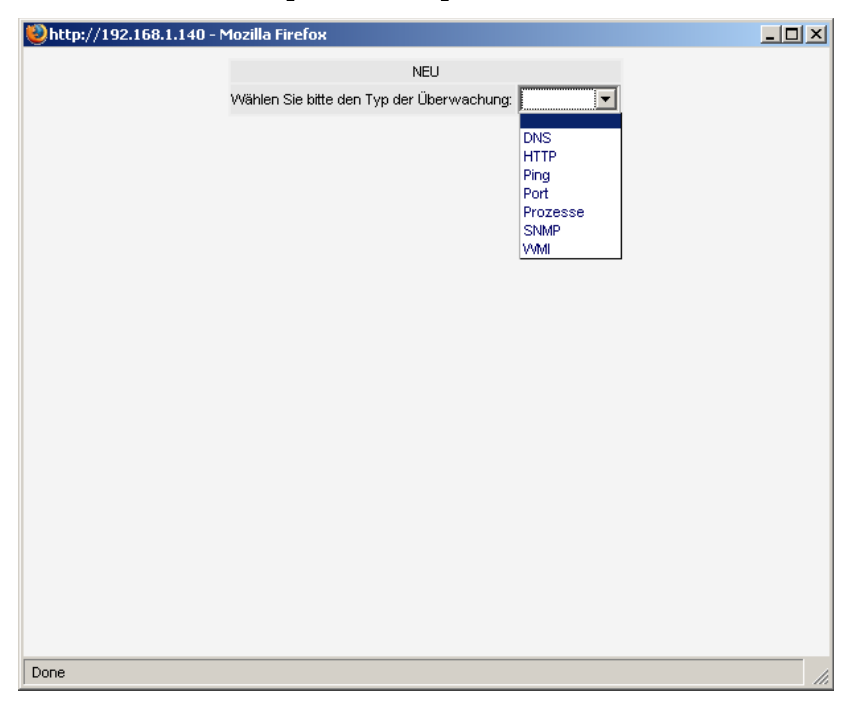


Abbildung 25: Auswahl der Methode eines Monitors

Im vorliegenden Release 1.3 werden die folgenden Methoden unterstützt:

- DNS
  Überwachung von DNS Servern
- HTTP
  Überwachung von http Servern, klassisch ist es der Port 80, kann aber auch jeder andere beliebige Port sein
- Ping
  Überwachung der Erreichbarkeit mittels Ping.
- Port
  Überwachung eines beliebigen TCP-Ports. UDP Ports lassen sich nicht damit überwachen.
- Prozesse
  Überwachung von Prozessen auf Desktop- oder Serversystemen
- SNMP
  Überwachung von beliebigen SNMP OID Objekten. SNMP steht

für Simple Network Management Protokoll und ist der weltweite Standard für die Überwachung von Netzwerk-, Desktop- und Serversystemen. SNMP ist auf allen Unix und allen neueren Windows Systemen (wird ab Windows 2000 mit auf der CD geliefert) verfügbar.

- WMI
  Überwachung von beliebigen WMI-Objekten. WMI steht für Windows Management Interface und ist auf nahezu jedem neueren Windows System verfügbar.

Mit diesen sieben Methoden sind umfangreiche Überwachungen möglich. Jeweils nach Auswahl einer Methode erscheinen unterschiedliche, für die jeweilige Methode spezifisch erstellte Konfigurationsfenster.

6.4.1 Methode DNS

Nachfolgend ist der Konfigurationsbildschirm der DNS Methode zu sehen:

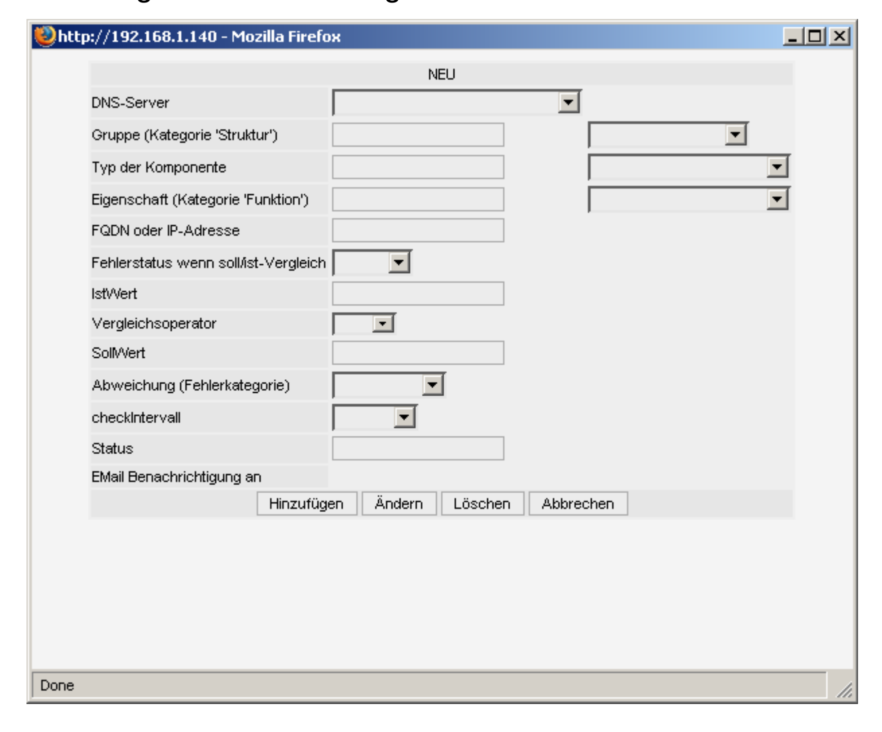


Abbildung 26: Konfiguration eines DNS Monitors

Zuerst muss das zu überwachende Objekt, in diesem Fall der DNS Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist auf Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur zu konfigurieren. Hier können Sie Freitext eingeben. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag „Typ der Komponente“ ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur DNS_Server ein, so können Sie hier z.B. Windows_Server oder Linux_Server eingeben. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte auch noch mal auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

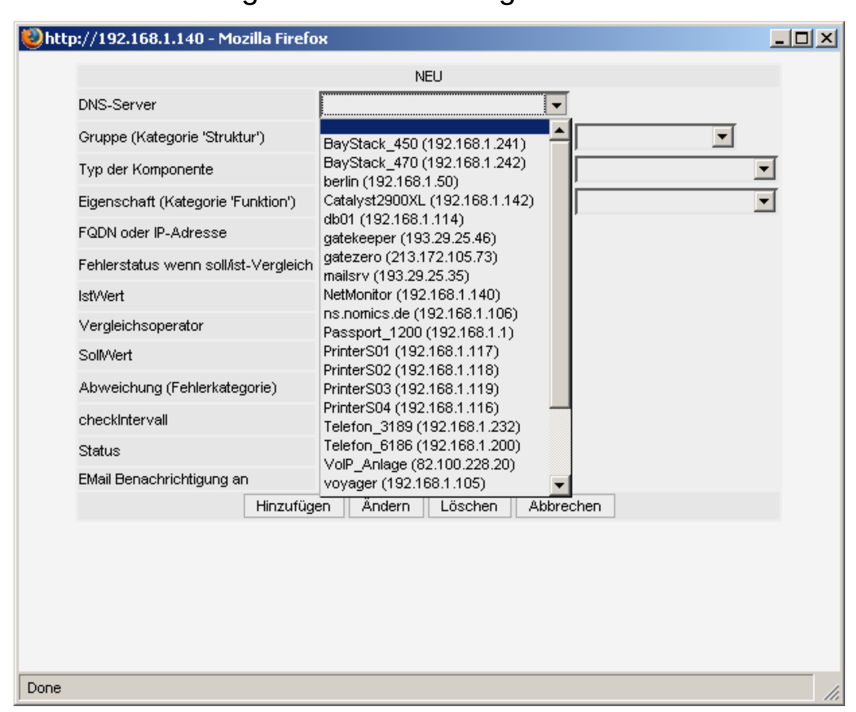


Abbildung 27: Auswahlfenster der konfigurierten Systeme

Darunter ist die Kategorie Funktion zu konfigurieren. Hier können Sie Freitext eingeben, z.B. DNS_Funktion. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist der FQDN oder der aufzulösende Hostnamen einzutragen. Logisch wird seitens des NetMonitors der obige Nameserver nach dem hier einzutragenden FQDN abgefragt und das Ergebnis in die Datenbank eingetragen.

Beim Fehlerstatus können Sie wählen zwischen „falsch“ und „wahr“.

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus „falsch“ oder „wahr“ reagieren. So können Sie für ein und die gleiche Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der „IST-Wert“ ist der seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des „Vergleichsoperators“ mit dem „Sollwert“ verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

- Ignorieren
  Es wird kein Event generiert
- Warning1
  Es wird ein Event mit dem Merkmal Warning 1 generiert
- Warning2
  Es wird ein Event mit dem Merkmal Warning 2 generiert
- Critical
  Es wird ein Event mit dem Merkmal „Critical“ generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem „Status“feld erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mailbenachrichtigung (siehe 6.4.1.1) eintragen.

6.4.1.1 Monitor spezifische E-Mailbenachrichtigung

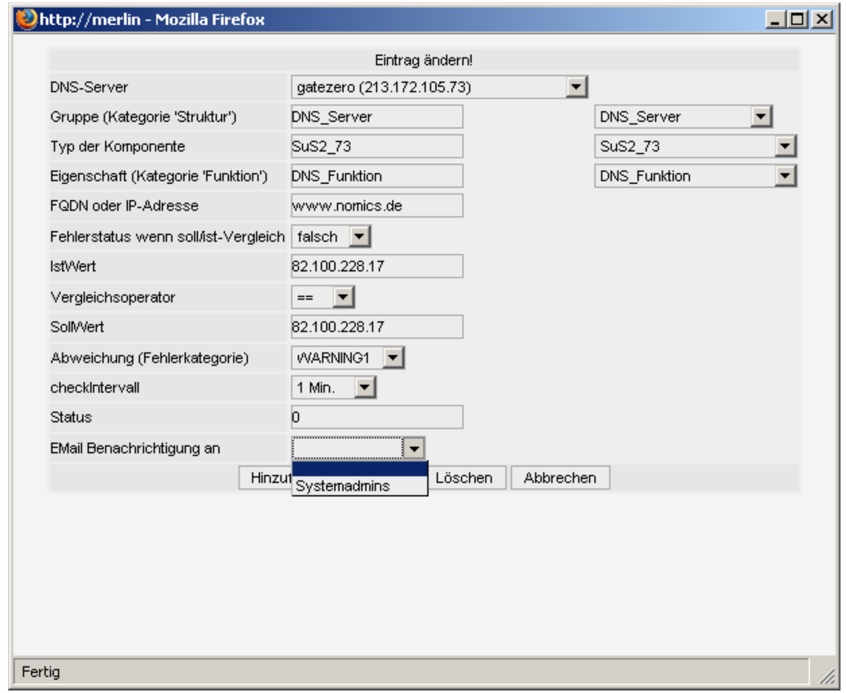


Abbildung 28: Konfiguration der Monitor spezifische E-Mailbenachrichtigung

Vorraussetzung für diese Konfiguration ist die Konfiguration einer entsprechenden Gruppe in der Benutzerverwaltung. Falls dort nichts konfiguriert ist, ist das Feld „Email Benachrichtigung an“ nicht nutzbar.

Falls die betreffenden Gruppe nicht konfiguriert wurde, so erscheint sie hier nicht im Auswahldialog.

In diesem Beispiel gibt es nur die Gruppe der Systemadministratoren. Daher würde in diesem Beispiel Events nur an Benutzer geschickt werden, die zum einen eine eingetragene E-Mailadresse haben und in der Gruppe der Systemadministratoren eingetragen sind.

6.4.2 Methode HTTP

Nachfolgend ist der Konfigurationsbildschirm der HTTP Methode zu sehen:

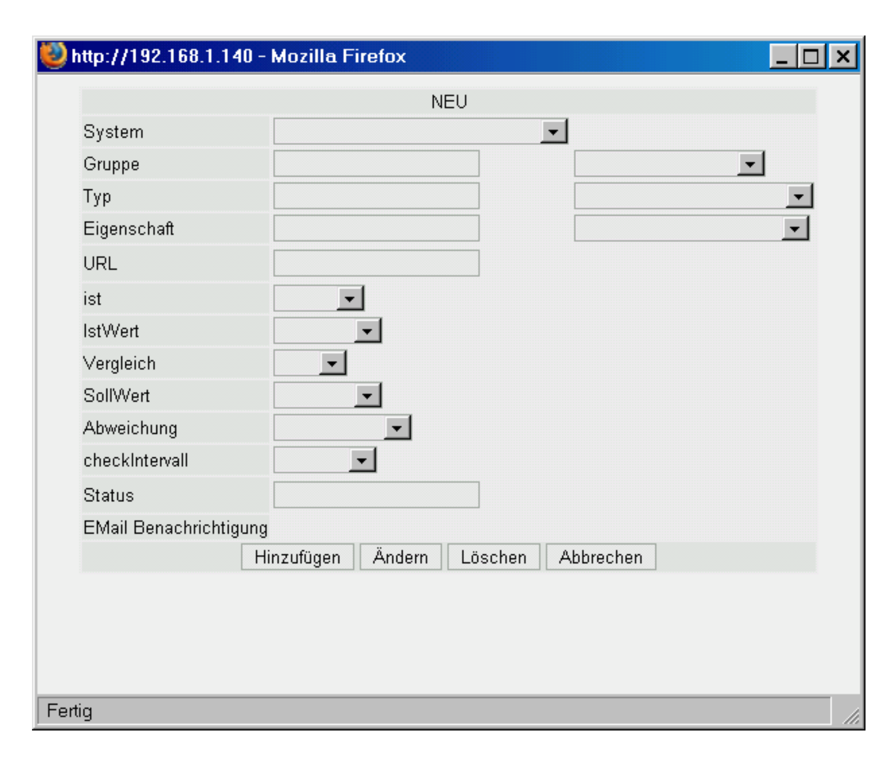


Abbildung 29: Konfiguration der http Methode

Zuerst muss das zu überwachende Objekt, in diesem Fall der HTTP Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur (in diesem Menü noch Gruppe genannt) zu konfigurieren. Hier können Sie Freitext eingeben. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag „Typ der Komponente“ ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur HTTP_Server ein, so können Sie hier z.B. Debian Sarge oder Linux_Server eingeben. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte nochmals auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion (in diesem Menü noch Eigenschaft genannt) zu konfigurieren. Hier können Sie Freitext eingeben, z.B. http_Funktion. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist die abzufragende URL einzutragen. Logisch wird seitens des NetMonitors der obige http-Server nach der hier einzutragenden URL abgefragt und das Ergebnis in die Datenbank eingetragen.

Beim Fehlerstatus können Sie wählen zwischen „falsch“ und „wahr“.

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus „falsch“ oder „wahr“ reagieren. So können Sie für ein und die gleiche Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der „IST-Wert“ ist das seitens des Monitors ermittelten Ergebnisses. Dieser wird mittels des „Vergleichsoperators“ mit dem „Sollwert“ verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

- Ignorieren
  Es wird kein Event generiert
- Warning1
  Es wird ein Event mit dem Merkmal Warning 1 generiert
- Warning2
  Es wird ein Event mit dem Merkmal Warning 2 generiert
- Critical
  Es wird ein Event mit dem Merkmal „Critical“ generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem „Statusfeld“ erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.3 Methode PING

Nachfolgend ist der Konfigurationsbildschirm der PING Methode zu sehen:

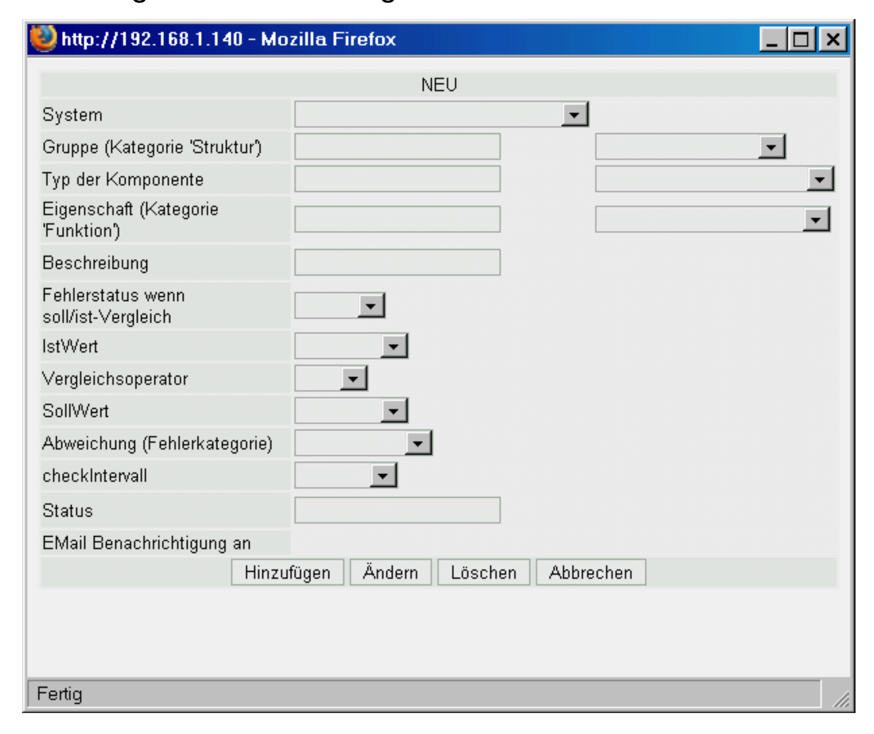


Abbildung 30: Konfiguration der Ping Methode

Zuerst muss das Objekt, in diesem Fall das zu überwachende Objekt, z.B. Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur (in diesem Menü noch Gruppe genannt) zu konfigurieren. Hier können Sie Freitext eingeben. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag „Typ der Komponente" ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur HTTP_Server ein, so können Sie hier z.B. Debian_Sarge oder Linux_Server eingeben. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte nochmals auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Erreichbarkeit. Dieser Freitext als logische

Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist eine Beschreibung einzutragen. Hiermit können Sie weitere Informationen verankern, z.B. als Beschreibung PING.

Beim Fehlerstatus können Sie wählen zwischen „falsch“ und „wahr“.

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus „falsch“ oder „wahr“ reagieren. So können Sie bei der Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der „IST-Wert“ ist das seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des „Vergleichsoperators“ mit dem „Sollwert“ verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

- Ignorieren
  Es wird kein Event generiert
- Warning1
  Es wird ein Event mit dem Merkmal Warning 1 generiert
- Warning2
  Es wird ein Event mit dem Merkmal Warning 2 generiert
- Critical
  Es wird ein Event mit dem Merkmal „Critical“ generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem „Status“feld erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.4 Methode Port

Nachfolgend ist der Konfigurationsbildschirm der Port Methode zu sehen:

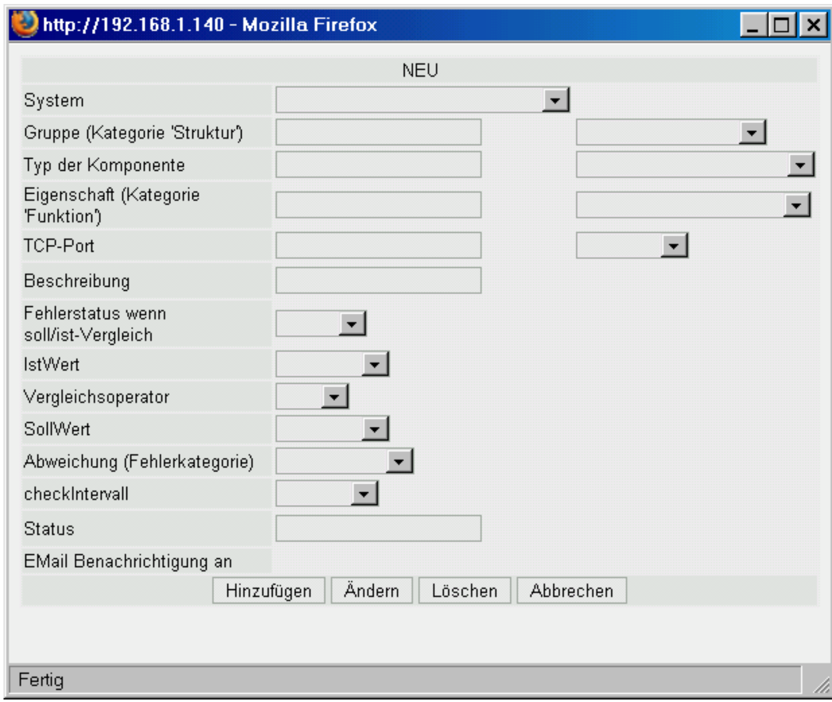


Abbildung 31: Konfiguration der Port Methode

Zuerst muss das zu überwachende Objekt, in diesem Fall der zu überwachende Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur zu konfigurieren. Hier können Sie Freitext eingeben. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag „Typ der Komponente“ ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur Applikations_Server ein, so können Sie hier z.B. Windows_2000_Server oder Linux_Server eingeben. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte auch noch mal auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion (in diesem Menü noch Eigenschaft genannt) zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Applikations_Funktion. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist der abzufragende Port einzutragen. Logisch wird seitens des NetMonitors der obige Server nach dem hier eingetragenen Port abgefragt und das Ergebnis in die Datenbank eingetragen.

Beim Fehlerstatus können Sie wählen zwischen „falsch“ und „wahr“.

Dieser Eintrag wirkt sich im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus „falsch“ oder „wahr“ reagieren. So können Sie bei der Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der „IST-Wert“ ist der seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des „Vergleichsoperators“ mit dem „Sollwert“ verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

- Ignorieren
  Es wird kein Event generiert
- Warning1
  Es wird ein Event mit dem Merkmal Warning 1 generiert
- Warning2
  Es wird ein Event mit dem Merkmal Warning 2 generiert
- Critical
  Es wird ein Event mit dem Merkmal „Critical“ generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem „Statusfeld“ erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.5 Methode Prozesse

Nachfolgend ist der Konfigurationsbildschirm der Prozess Methode zu sehen:

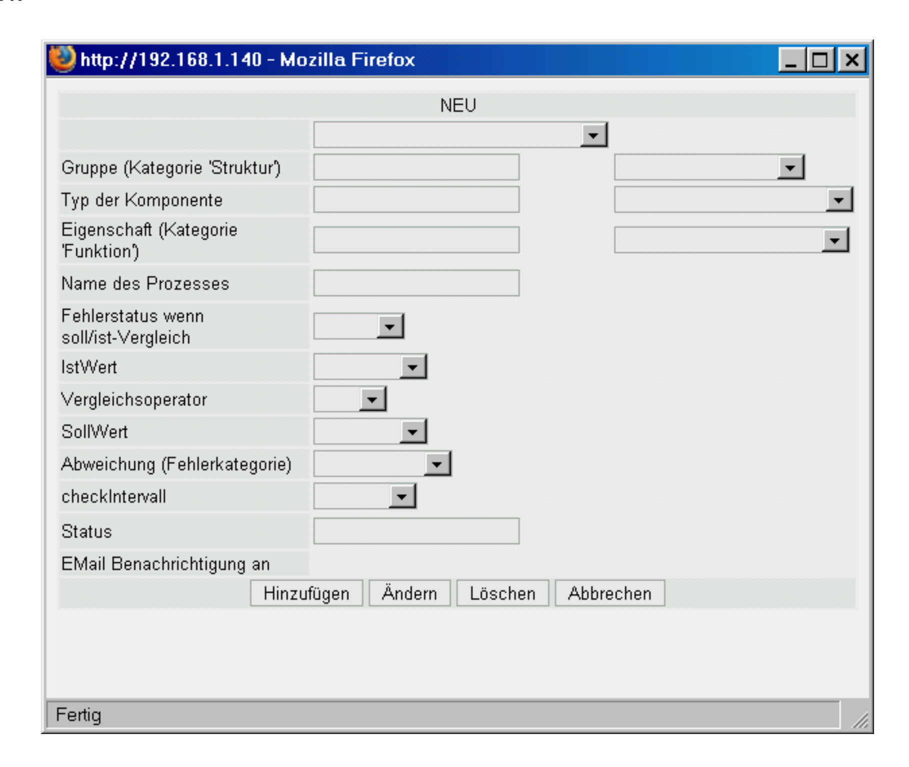


Abbildung 32: Konfiguration der Prozess Methode

Zuerst muss das zu überwachende Objekt, in diesem Fall der zu überwachende Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Windows_Server. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag „Typ der Komponente“ ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur Applikations_Server ein, so können Sie hier z.B. Windows_2000_Server oder Windows_NT. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte auch noch mal auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion (in diesem Menü noch Eigenschaft genannt) zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Anti_Viren_Funktion. Dieser Freitext als logische Ordnungsgruppe

erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist der abzufragende Prozess einzutragen. Logisch wird seitens des NetMonitors der obige Server nach dem hier eingetragenen Prozess abgefragt und das Ergebnis in die Datenbank eingetragen. Bei Windows Systemen wird dies durch eine TaskListen Afrage durchgeführt. Bei Unix-Systemen wird eine Prozesstabellenabfrage durchgeführt.

Beim Fehlerstatus können Sie wählen zwischen „falsch“ und „wahr“.

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus „falsch“ oder „wahr“ reagieren. So können Sie bei der Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der „IST-Wert“ ist das seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des „Vergleichsoperators“ mit dem „Sollwert“ verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

- Ignorieren
  Es wird kein Event generiert
- Warning1
  Es wird ein Event mit dem Merkmal Warning 1 generiert
- Warning2
  Es wird ein Event mit dem Merkmal Warning 2 generiert
- Critical
  Es wird ein Event mit dem Merkmal „Critical“ generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem „Status“feld erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.6 Methode SNMP

Nachfolgend ist der Konfigurationsbildschirm der SNMP Methode zu sehen:

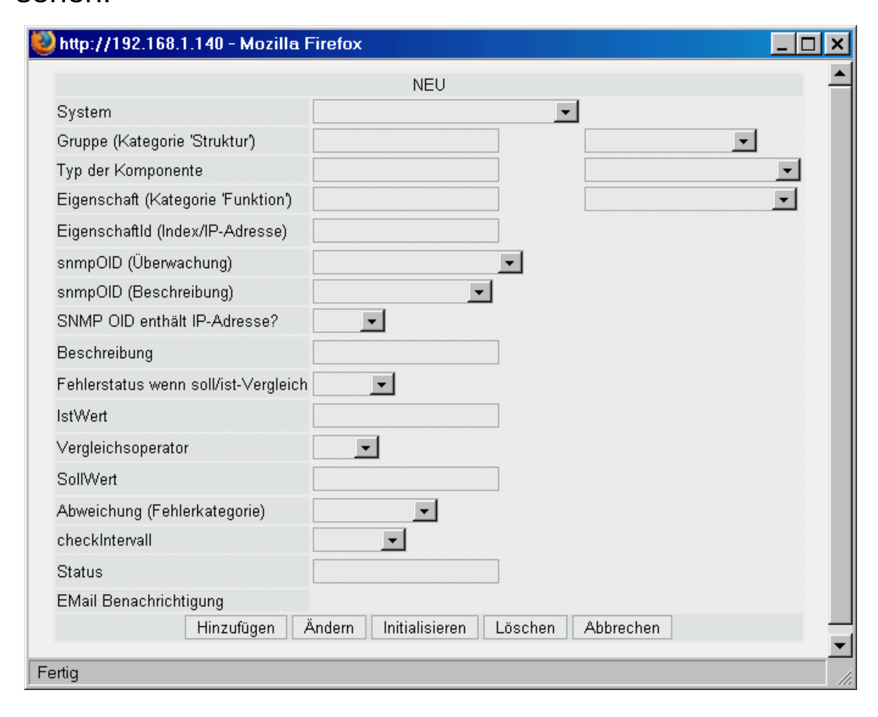


Abbildung 33: Konfiguration der SNMP Methode

Zuerst muss das zu überwachende Objekt, in diesem Fall der zu überwachende Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Linux_Server. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag "Typ der Komponente" ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur Linux_Server ein, so können Sie hier z.B. Debian_Sarger oder HPUX_11 eintragen. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte auch noch mal auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion (in diesem Menü noch Eigenschaft genannt) zu konfigurieren. Hier können Sie Freitext eingeben, z.B. SNMP_Funktion. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist der abzufragende Prozess einzutragen. Logisch wird seitens des NetMonitors der obige Server nach dem hier eingetragenen SNMP OID Objekt abgefragt und das Ergebnis in die Datenbank eingetragen. Die ist auch bei Windows Systemen möglich, da ab Windows 2000 der SNMP Server auf der Installationsmedium mitgeliefert wird.

Beim Fehlerstatus können Sie wählen zwischen "falsch" und "wahr".

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus "falsch" oder "wahr" reagieren. So können Sie bei der Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der "IST-Wert" ist das seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des "Vergleichsoperators" mit dem "Sollwert" verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

· Ignorieren

Es wird kein Event generiert

· Warning1

Es wird ein Event mit dem Merkmal Warning 1 generiert

· Warning2

Es wird ein Event mit dem Merkmal Warning 2 generiert

· Critical

Es wird ein Event mit dem Merkmal "Critical" generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem "Status"feld erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.7 Methode WMI

Nachfolgend ist der Konfigurationsbildschirm der WMI Methode zu sehen:

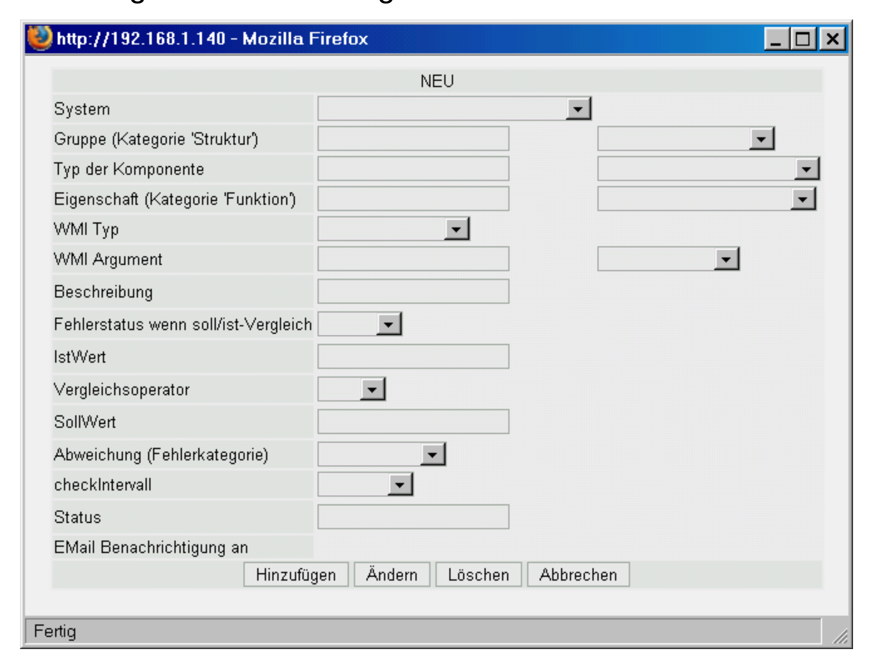


Abbildung 34: Konfiguration der WMI Methode

Zuerst muss das zu überwachende Objekt, in diesem Fall der zu überwachende Server, im Menü Systems konfiguriert worden sein. Wenn er dort konfiguriert wurde, so taucht er auch in dem Auswahlmenü auf. Dies ist in Abbildung 27 zu sehen.

Darunter ist die Kategorie Struktur zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Windows_Server. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Struktur Darstellung.

Der Eintrag "Typ der Komponente" ermöglicht eine tiefere Unterscheidung dieser logischen Ordnungsgruppe. Tragen Sie z.B. bei Struktur Windows_Server ein, so können Sie hier z.B. Windows_2000 oder Windows_XP. Der Typ der Komponente taucht später in der Aufteilung der Struktur Objekte auch noch mal auf.

Wichtig: Bitte keine Bindestriche in der Namensbezeichnung eingeben. Im vorliegenden Release erzeugt dies noch unter gewissen Datenbankabfragen Fehlermeldungen.

Darunter ist die Kategorie Funktion (in diesem Menü noch Eigenschaft genannt) zu konfigurieren. Hier können Sie Freitext eingeben, z.B. Hauptspeichernutzung. Dieser Freitext als logische Ordnungsgruppe erscheint dann zukünftig im rechten Auswahlmenü und ebenso im Überwachungsbildschirm in der Funktion Darstellung.

Nachfolgend ist der abzufragende Prozess einzutragen. Logisch wird seitens des NetMonitors der obige Server nach dem hier eingetragenen WMI Objekt abgefragt und das Ergebnis in die Datenbank eingetragen. WMI ist, wie der Name sagt ein Windows Management Interface und stellt, abhängig vom Betriebssystem sehr viele Abfragemöglichkeiten zur Verfügung. Ähnlich wie bei SNMP kann so ziehmlich jeder beliebige Betriebszustand abgefragt werden. Ebenso, wie bei SNMP, muss ein Agent (Management Interface) installiert sein, welches die Abfragen entgegen nimmt und innerhalb des Windows System umsetzt.

Beim Fehlerstatus können Sie wählen zwischen "falsch" und "wahr".

Dieser Eintrag wirkt sich logisch im Eventhandling auf die nachfolgende Bedingung aus. Ist die Bedingung erfüllt, so kann der zu erzeugende Event auf den Fehlerstatus "falsch" oder "wahr" reagieren. So können Sie bei der Überwachung abhängig vom Ergebnis unterschiedlich reagieren, z.B. eine Mail verschicken oder einen entsprechenden Status im Überwachungsbildschirm schalten.

Der "IST-Wert" ist der seitens des Monitors ermittelten Ergebnisses. Dieses wird mittels des "Vergleichsoperators" mit dem "Sollwert" verglichen.

Die Abweichung, bzw. Severity ermöglicht eine Unterscheidung, wie kritisch dieser Monitor ist. Sie können wählen zwischen

· Ignorieren

Es wird kein Event generiert

· Warning1

Es wird ein Event mit dem Merkmal Warning 1 generiert

· Warning2

Es wird ein Event mit dem Merkmal Warning 2 generiert

· Critical

Es wird ein Event mit dem Merkmal "Critical" generiert

Mit der Auswahlbox stellen Sie den Überwachungszyklus des Monitors ein. Sie können von 1 Minute bis zu 30 Minuten einstellen. Sinnvolle Überwachungszeiten liegen zwischen 5 und 10 Minuten. Abhängig von der Methode sind unterschiedlich viele Datenbankoperationen notwendig, welche bei vielen unterschiedlichen Monitoren Rechnerleistung benötigen.

In dem "Status"feld erscheint der aktuelle Überwachungsstatus des Monitors. Dieser Wert wird vom Monitor eingetragen, daher brauchen Sie ihn nicht konfigurieren. Falls notwendig können Sie den Status löschen, dann wird er beim nächsten Überwachungszyklus wieder eingetragen.

Zum Schluss können Sie noch eine Monitor spezifische E-Mail-Benachrichtigung (siehe 6.4.1.1) eintragen.

6.4.8 Zusammenfassung

Feld	Beschreibung
System	System, welches geprüft werden soll aus Liste auswählen
Gruppe	Gruppe eintragen/auswählen --> dient der Gliederung in GUI
Typ	Typ eintragen/auswählen --> dient der Gliederung in GUI
Eigenschaft	Eigenschaft eintragen/auswählen --> dient der Gliederung in GUI
EigenschaftId	Abhägig vom checkType dient dieser als Wert zu speziefizierung des abzufragendenObjekts z.B. SNMP: Index des abzufragenden Interfaces z.B.: Port: Port, welcher per tcp auf aktivität geprüft werden soll
snmpUid	Snmp-Uid, welche per snmp abgefragt wird. An diese wird bei Abfrage EigenschaftId angehängt
SnmpBeschreibung	Snmp-uid, welche bei Initialisierung des Systems genutzt wird, um die Beschreibung für das objekt zu erhalten
IndexIstIp	Nur bei SNMP: wenn EigenschaftId eine als Integer gespeicherte IP-Adresse ist, dann „Ja“. z.B. wenn routingtable abgefragt werden soll
Beschreibung	Text, welcher das Objekt beschreibt z.B. „Port 1 Slot 1“
Ist	- ist WAHR/FALSCH gibt an, ob die folgende Bedingung WAHR bzw, FALSCH sein soll, um den Status zu setzen und Emails zu versenden. Bsp.: WAHR (ist Wert(???) == sollWert (10)) --> CRITICAL, EMAIL in diesem Fall wird der Status CRITICAL gesetzt und eine EMAIL versendet, wenn istWert gleich 10

Feld	Beschreibung
	ist. Denn: 10 == 10 ist wahr FALSCH (istWert(???) == sollWert (10)) --> CRITICAL, EMAIL in diesem Fall wird der Status CRITICAL gesetzt und eine EMAIL versendet, wenn istWert ungleich 10 ist. Denn: 9 == 10 ist falsch
IstWert	Der aktuelle Wert des Objekts
Vergleich	Vergleichsoperator zur Ermittlung eines Status
SollWert	wird als Referenzwert genutzt
Abweichung	gibt an, welchen Status das Objekt einnimmt, wenn der Vergleich zwischen is tWert und Soll Wert nicht WAHR ist.
CheckIntervall	definiert, wie oft ein Objekt geprüft werden soll
Status	Zeigt den aktuellen Status des Objekts
Email Benachrichtigung	gibt an, welche Gruppe (Benutzer) durch Emails benchrichtigt werden sollen.
FQDN / IP	Fqdn bzw. ip-adresse, welche per dns aufgelöst werden soll

6.5 Andere

Im Laufe der „Global“-Konfiguration werden Sie feststellen, das das Menü unter Einstellungen wächst.

Es werden für alle „SystemGruppen“ weitere Menüs angelegt. Unter diesen finden Sie dann alle zu diesen Gruppen gehörenden Ssteme, welche Sie dann wiederum zu deren Objekten führen.

Der wesentliche Unterschied zur globalen Konfiguration ist, dass an dieser Stelle keine Objekte angelegt oder gelöscht werden können.

Es können lediglich folgende Werte geändert bzw. angepasst werden:

- Vergleich

welche Funktion soll zum Vergleich des aktuellen Wertes (ist Wert) mit dem Referenz-Wert „Sollwert“ genutzt werden

- Soll Wert

  wird als ReferenzWert genutzt

- CheckIntervall

  definiert, wie oft ein Objekt geprüft werden soll

- Abweichung

  gibt an, welchen Status das Objekt einnimmt, wenn der Vergleich zwischen ist Wert und Soll Wert nicht WAHR ist.

- send Mail To
  gibt an, welche Gruppe (Benutzer) durch Emails benachrichtigt werden sollen.

7 Log

Unter diesem Menüpunkt werden die Logfile spezifischen Aktionen zu sammen gefaßt.

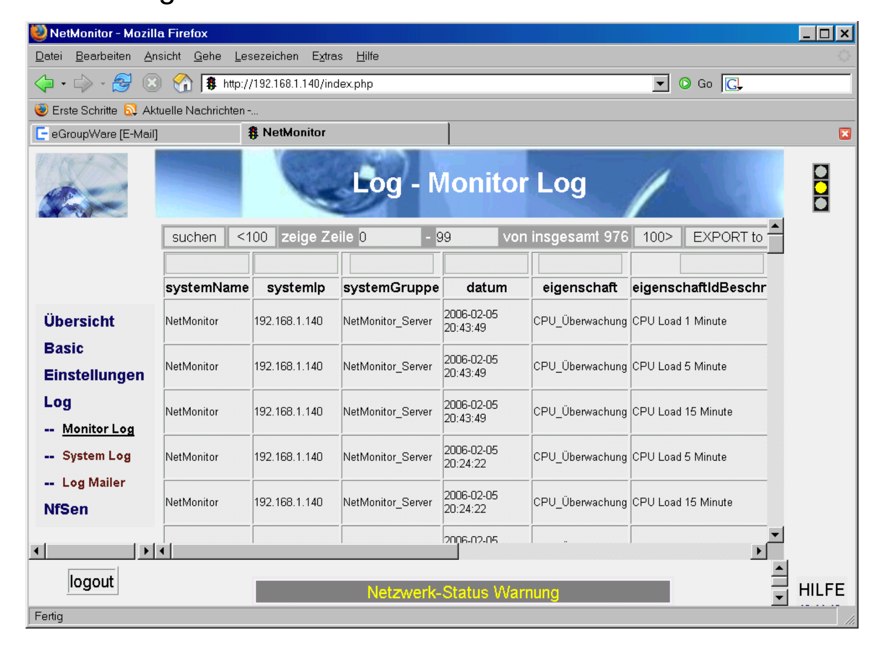


Abbildung 35: Log Menü

Auf der linken Seite in der obigen Abbildung in das aufgeblendete Log Menü zu sehen.

7.1 Monitor Log

Im Hauptbildschirm von Abbildung 30 ist die Administration des Monitor Logs zu sehen. Mit Monitor Log werden an dieser Stelle die Logfiles des NetMonitors gemeint.

Werden seitens eines Monitors die gesetzten Bedingungen nicht erfüllt oder weichen sie vom konfigurierten Status ab, so wird ein entsprechender Eintrag im Monitor Log vorgenommen.

Alle relevanten Informationen werden hierbei in das Monitor Log geschrieben.

Innerhalb des Log Menüs kann beliebig gesucht werden. Hierzu muss nur das entsprechende Objekt in die Suchleiste eingetragen werden. Siehe hierzu Abbildung 31 (oben links mir den Fragezeichen).
In jeder Spalte vom Log Menü ist diese Suche möglich (innerhalb der vorhandenen Datenbank) und somit wird der Suchzeitraum nur von der physikalischen Größe der Datenbank bestimmt.

Ein Export in eine CSV Tabelle ist ebenso über das Log Menü möglich. Hierzu ist es nur notwendig oben rechts das entsprechende Feld anzuklicken. Danach öffnet sich ein Dialogfeld, indem eine Abfrage bezüglich des Speicherplatzes erscheint oder die Daten direkt in z.B. Excel geladen werden können.

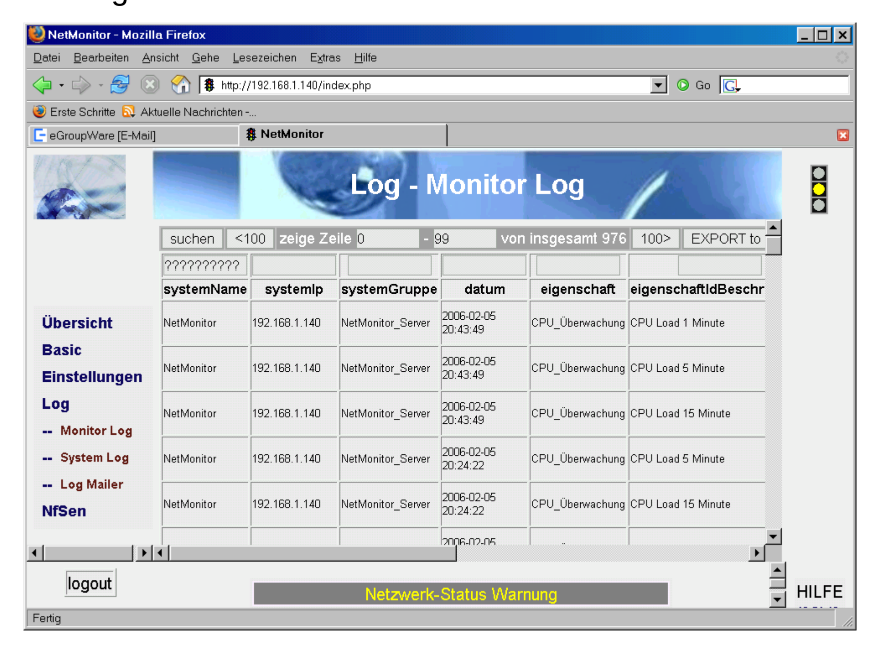


Abbildung 36: Suchfunktion im Log Menü

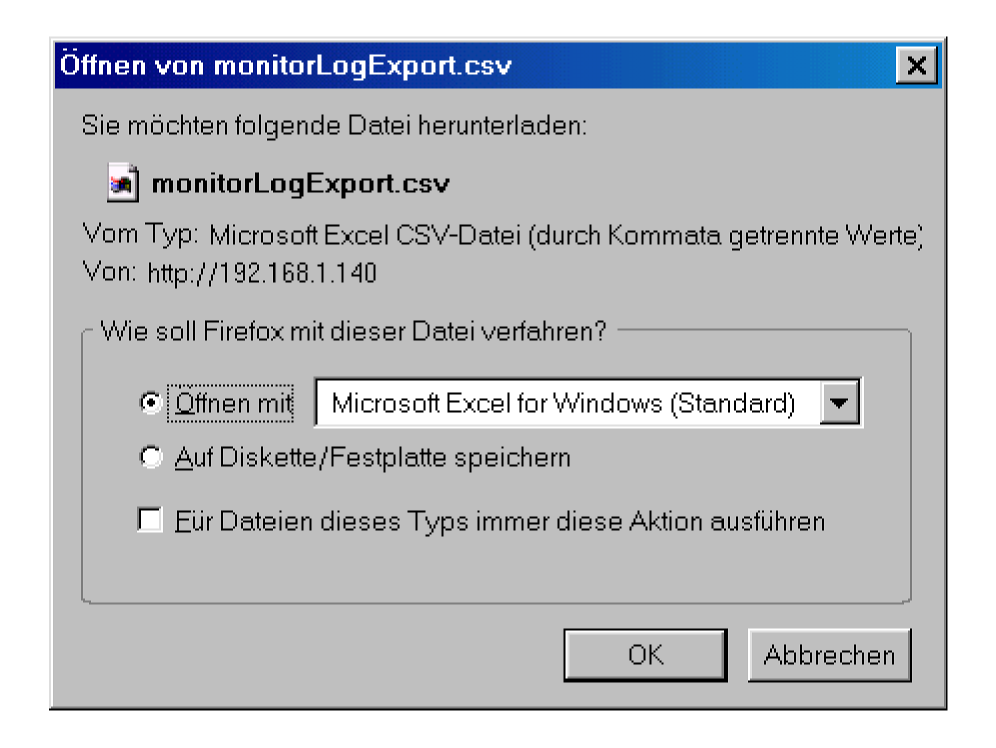


Abbildung 37: Export der Log Datei

7.2 System Log

Mit dem Menü System Log lassen sich weitere Logfiles, welche auf dem NetMonitor gespeichert oder verarbeitet werden sollen, untersuchen.

Hierzu werden „reale Ausdrücke“ eingesetzt.

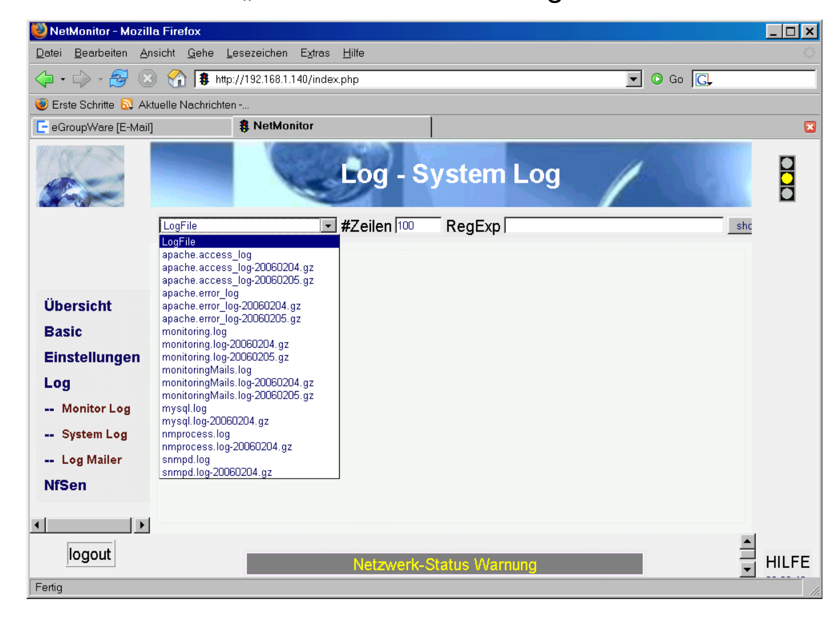


Abbildung 38: System Log

Zuerst wird auf der linken Seite das entsprechende Logfile markiert und danach oben rechts unter RegExp die realen Ausdrücke eingetragen. Mit Bestätigung wird dieses Logfile gemäß der Anweisung untersucht,. Das Ergebnis wird anschließend direkt angezeigt (siehe Abbildung 34).

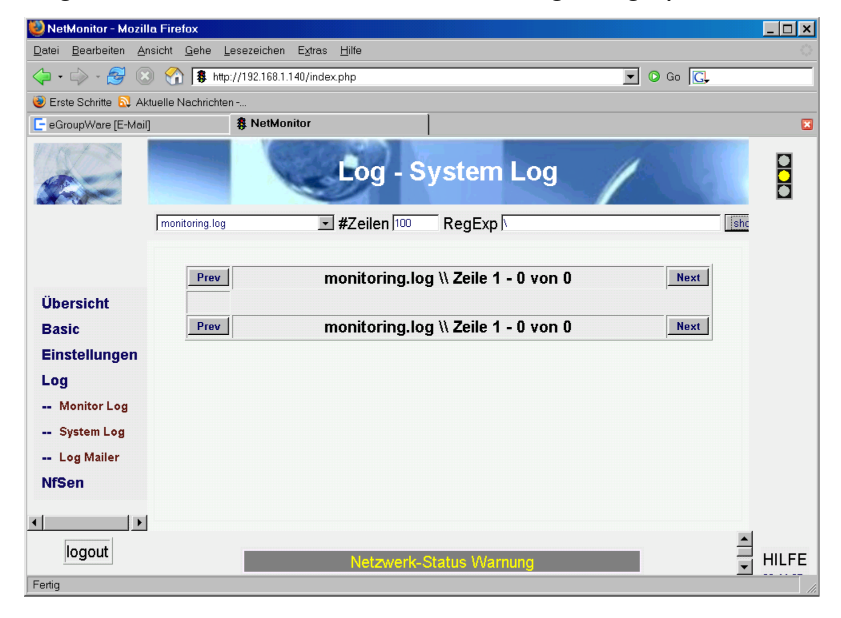


Abbildung 39: Ergebnis einer Abfrage im System Log

7.3 Log Mailer

Der Log Mailer ist eine direkte Ergänzung des System Log. Mit dem Log Mailer können Logfiles mittels realer Ausdrücke auf relevante Events untersucht werden.

Tritt ein solcher Event auf, so kann durch den Log Mailer eine Aktion durchgeführt werden. Hiermit können automatische Konfigurationsänderungen auf spezielle Anlässe realisieret werden.

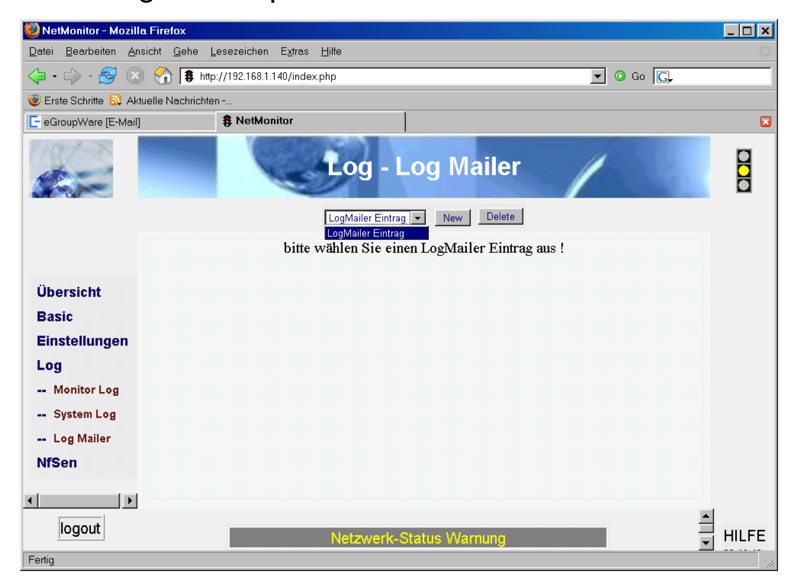


Abbildung 40: Log Mailer

Abbildung 34 zeigt den Konfigurationsdialog des Log Mailer. Zuerst wird ein Name für die auszuführende Operation eingetragen. Danach der jeweilige, reguläre Ausdruck, der E-Mail Empfänger und ein Text für die E-Mail.

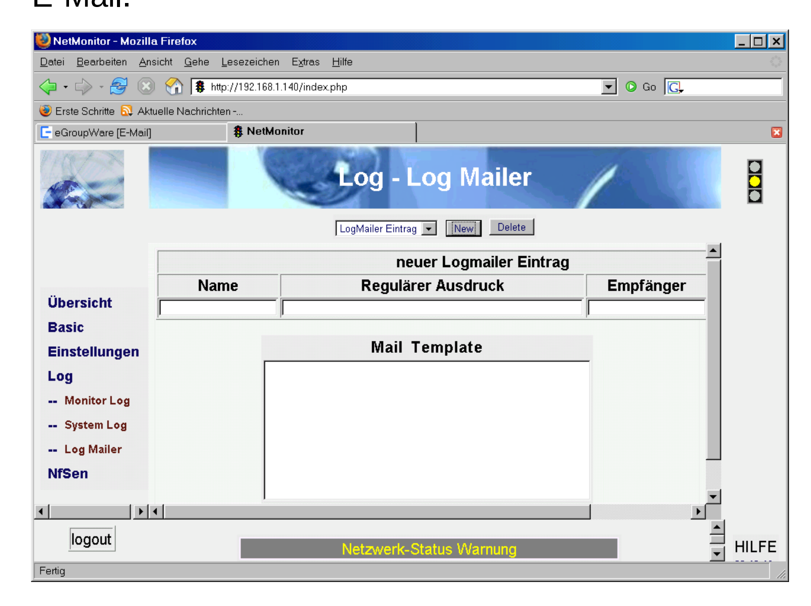


Abbildung 41: Konfiguration des Log Mailer

8 NFSen

NFSen ist Open Source und ein Traffic Analyse Werkzeug. Der Name kommt von **Net**F**low** **Sen**sor.

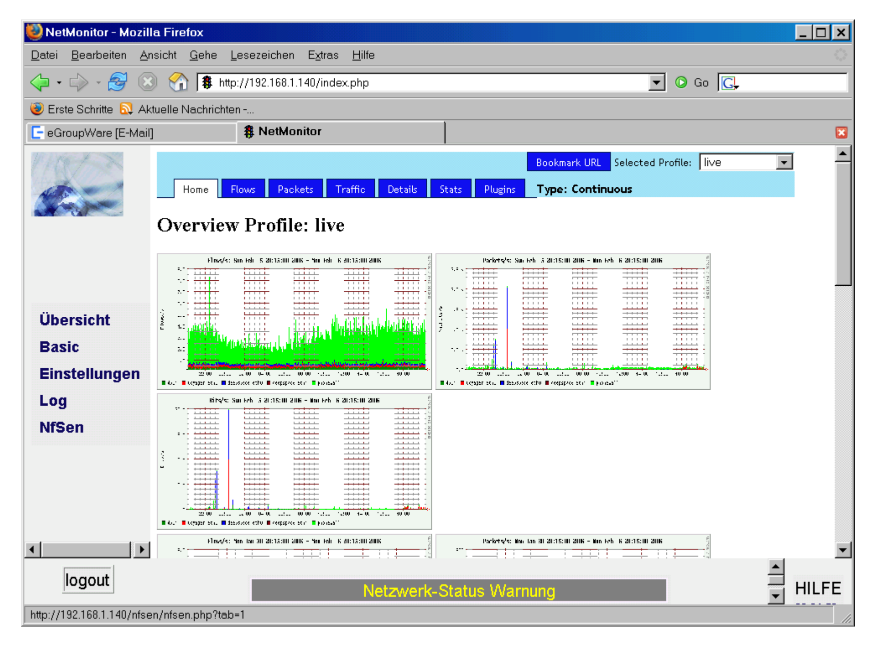


Abbildung 42: Informationsbildschirm von NFsen

Mit NFSen lassen sich die im Netzwerk vorhandenen Datenströme darstellen, visualisieren und analysieren.

NFSen ermöglicht:

- Darstellen von netflow Daten: Flows, Packets und Bytes
- Einfaches navigieren zwischen den netflow Daten
- Auswerten der netflow Daten in spezifischen Zeitslots
- Historie- und Laufzeitprofile
- Einfache Anpassung an die jeweiligen Umgebungen

8.1 NFSen Übersichtsbildschirm

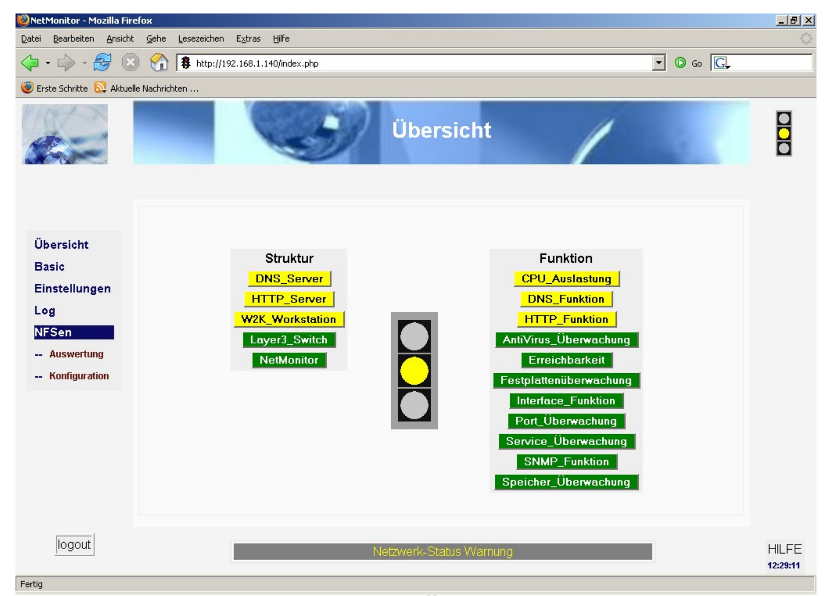


Abbildung 43: Übersichtsbildschirm von NFsen

Die obige Abbildung zeigt den Übersichtsbildschirm von NFSen. Mit Aufruf von NFSen im Menü auf der rechten Seite bleibt der aktuelle Bildschirminhalt unverändert und es werden im Menü die Menüoptionen von NFSen aufgeblendet.

- NFSen Auswertung
- NFSen Konfiguration

8.2 NFSen Auswertung

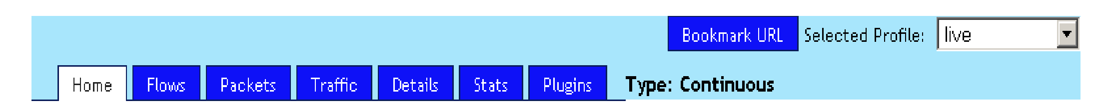
Mit Aufruf der NFSen Auswertung gelangt man auf den Startbildschirm



Abbildung 44: Startbildschirm von NFsen

NFSen. NFSen ist ein Open Source Produkt, welches wir nur eingebunden haben. Daher sind auch aktuell noch die Menüpunkte in Englisch ausgeführt.

In der nachfolgenden Abbildung ist die Menüleiste zu sehen. Aus dem Startbildschirm gelangen Sie jeweils über das Menü in die Darstellung von Flows (Kommunikation zwischen zwei Systemen), Packet, Traffic, Details, Stats und Plugins.



Overview Profile: live

Abbildung 45: Menüleiste von NFsen

Die Auswertequalität geht von links nach rechts in der Menüleiste. Über Plugins kann man sehr, sehr tief in die Auswertung gehen. Um die nachfolgenden Darstellungen zu verstehen ist es wichtig, hier an dieser Stelle auf das grundsätzliche Konzept von NFSen bzw. NetMonitor und NFSen einzugehen.

NFSen und Nomics NF-Probe

NFSen ist als eigenständige Applikation in den NetMonitor integriert und unterstützt die Cisco NetFlow Formate und die Nomics NF-Probe.

Die Nomics NF-Probe wird als externe Auswerteeinheit an Layer 2 oder Layer 3 Switche installiert, welche nicht das NetFlow Format beherrschen.

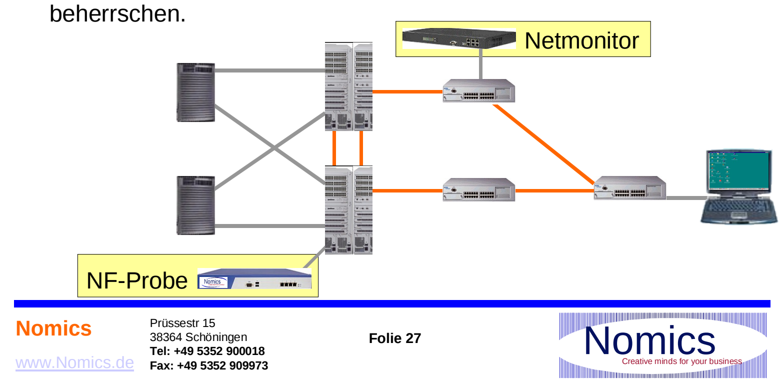


Abbildung 46: Integrationskonzept NetMonitor und NFSen

NetFlow ist ein durch Cisco entwickeltes Protokoll mit dem Information über den aktuellen Traffic an einem definierten System übergeben werden kann.

Layer 3 Switche von isco, z.B. Catalyst 6509 beherrschen das NetFlow Protokoll und können so Information über den Traffic, welche über diesen Switch geht an zentrale Managementsysteme zur Verfügung stellen. In

dem Switch werden Informationen gesammelt, wer mit wem welche Daten ausgetauscht hat. Dies wird auf Protokoll und Socket Ebene durchgeführt. Anhand dieser Informationen kann dann gesagt werden, das der Client mit der IP Adresse 192.168.1.50 mit dem http Server mit der IP Adresse 192.168.1.140 auf Basis des Protokolls HTTP 86 Kbyte Daten zu einem definierten Zeitpunkt ausgetauscht hat.

An jedem Switch, welches NetFlow beherrscht kann als Zieladresse der NetMonitor angegeben werden und so kann am NetMonitor der Traffic von diesem System ausgewertet werden. Aus Sicht des NetMonitors ist der Catalyst 6509 zu diesem Zeitpunkt eine Analyseeinheit, eine sogenannte Probe. Diese Probes werden in der NFSen Konfiguration durchkonfiguriert. Dazu aber später mehr.

8.2.1 NFSen Auswertung Flows

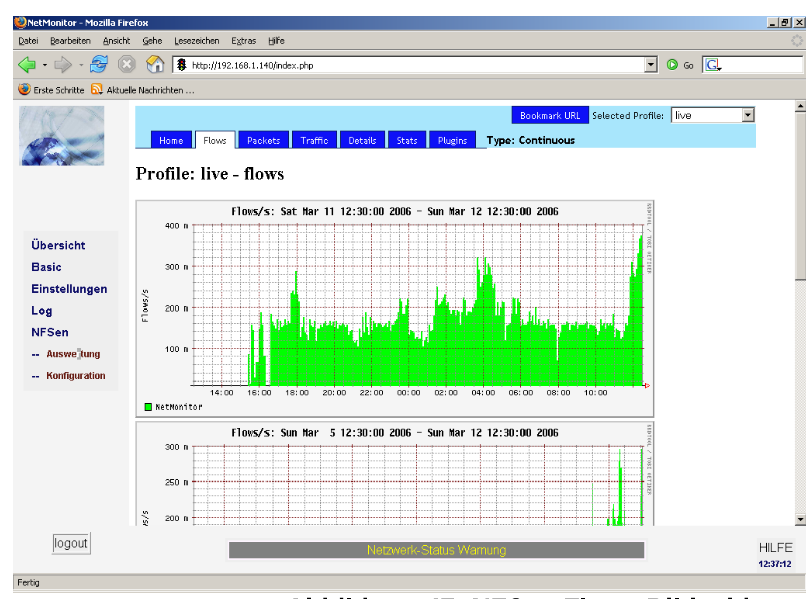


Abbildung 47: NFSen Flows Bildschirm

Mit Aufruf von Flows aus der NFSen Menüleiste gelangt man in die Auswertung der Flows. Dies zeigt die obige Abbildung 42.

Flows muss man in diesem Bildschirm in Beziehung zu den eben angesprochenen Probes setzen. Zu sehen ist dies in der Abbildung 43.

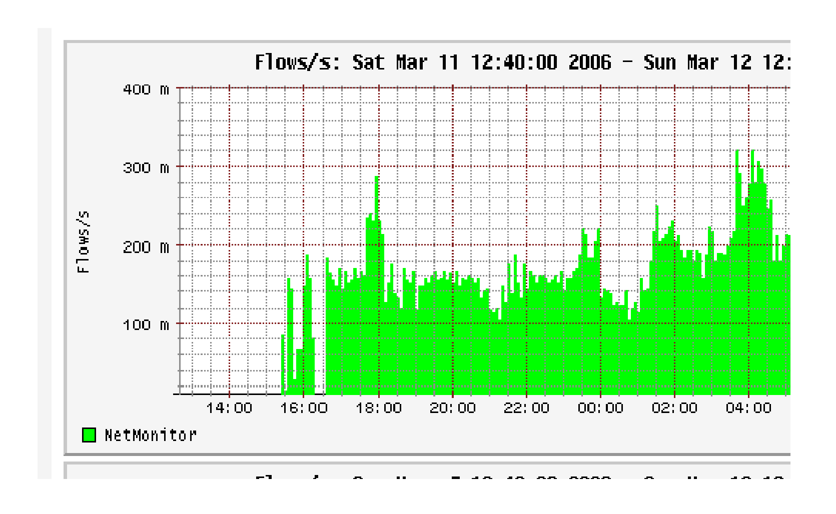


Abbildung 48: NFSen Flows Bildschirm

Deutlich ist in der Abbildung 43 unten links in der Ecke das grüne Kästchen mit der Beschriftung NetMonitor zu sehen. Der NetMonitor ist hier in diesem Beispiel als Probe konfiguriert worden. Zu sehen ist daher in diesem Bildschirm nur die Flow-Auswertung vom NetMonitor selbst.

In der nachfolgenden Darstellung ist ein anderes Beispiel zu sehen.

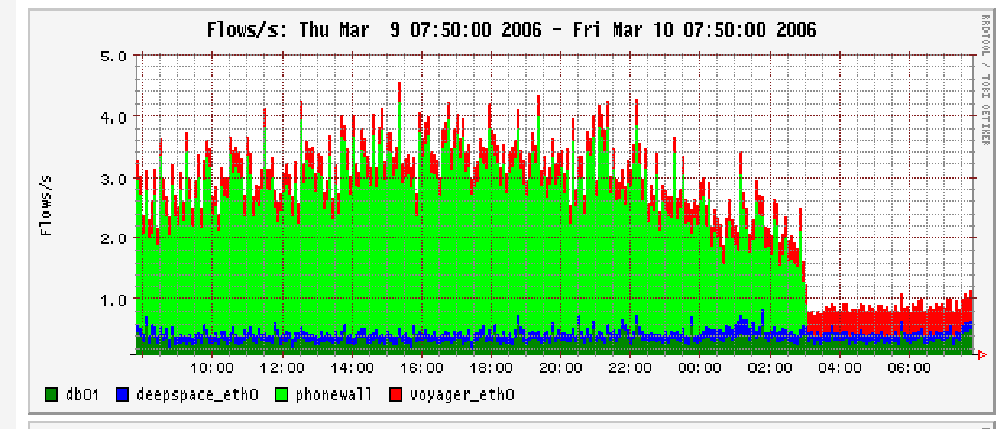


Abbildung 49: NFSen Flows Bildschirm, weiteres Beispiel

In diesem Beispiel sind vier Probes konfiguriert. Jede Probe ist über eine jeweils eigene Farbe zu erkennen. Gut zu sehen ist, das von der Probe „PhoneWall“ ab ca. 2.30 Uhr kein Traffic mehr zu sehen ist.

8.2.2 NFSen Auswertung Packets



Abbildung 50: NFSen Packets

Im Packets Bildschirm bekommt man tiefergehende Informationen zu der Probe. In dem Fall sehen wir Pakete/Sekunde, welche von der Probe aufgezeichnet wurden.

In vier Grafiken werden die jeweiligen Werte auf Basis einer Tages-, Wochen-, Monats- und Jahresbewertung dargestellt.

8.2.3 NFSen Auswertung Traffic

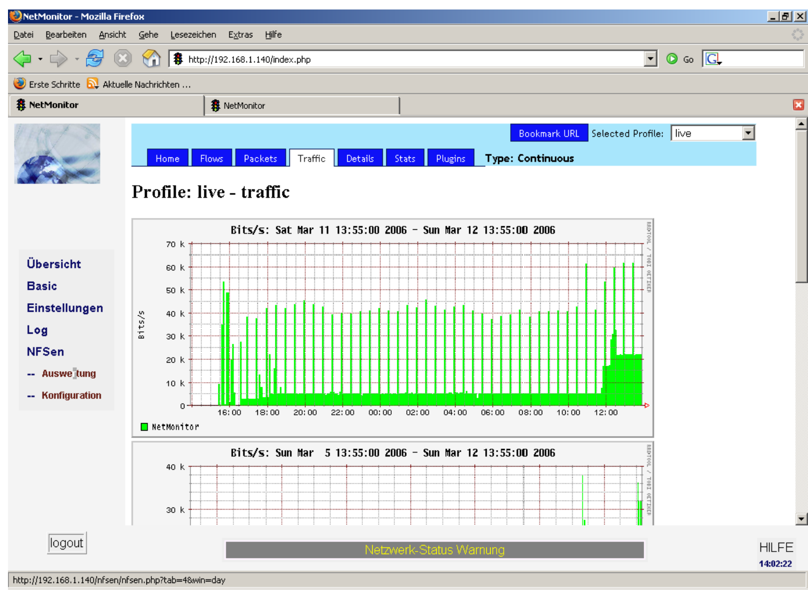


Abbildung 51: NFSen Traffic

Im Traffic Bildschirm bekommt man tiefergehende Informationen zu der Probe. In dem Fall sehen wir Bits/Sekunde, welche von der Probe aufgezeichnet wurden.

In vier Grafiken werden die jeweiligen Werte auf Basis einer Tages-, Wochen-, Monats- und Jahresbewertung dargestellt.

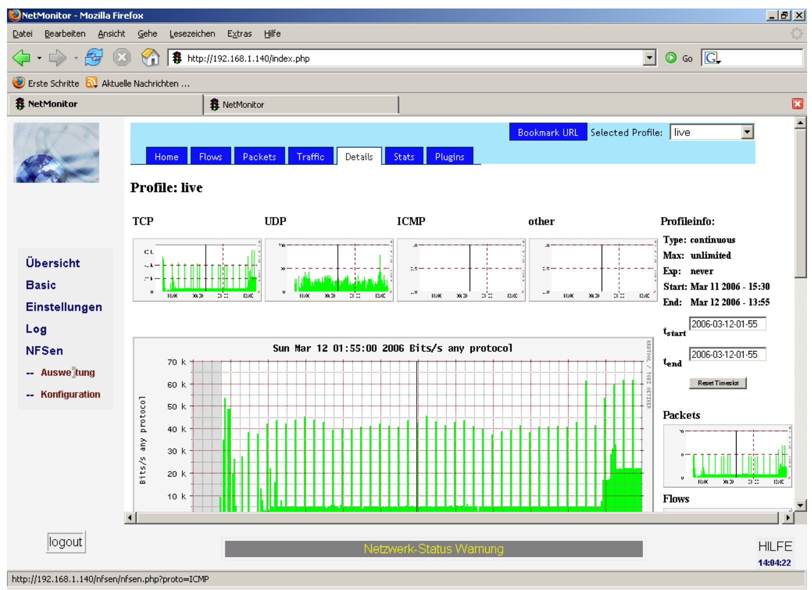


Abbildung 52: NFSen Details

8.2.4 NFSen Auswertung Details

Im NFSen Details Bildschirm wird eine sehr tief gehende Untersuchung des Traffics ermöglicht.

Im Prinzip laufen hier alle Informationen zusammen und können entsprechend den Notwendigkeiten analysiert werden. Unterschieden wir grundsätzlich in TCP, UDP, ICMP und andere Trafficarten. Wobei grundsätzlich bei diesen vier zwischen einer Flow- und Trafficanalyse unterschieden wird.

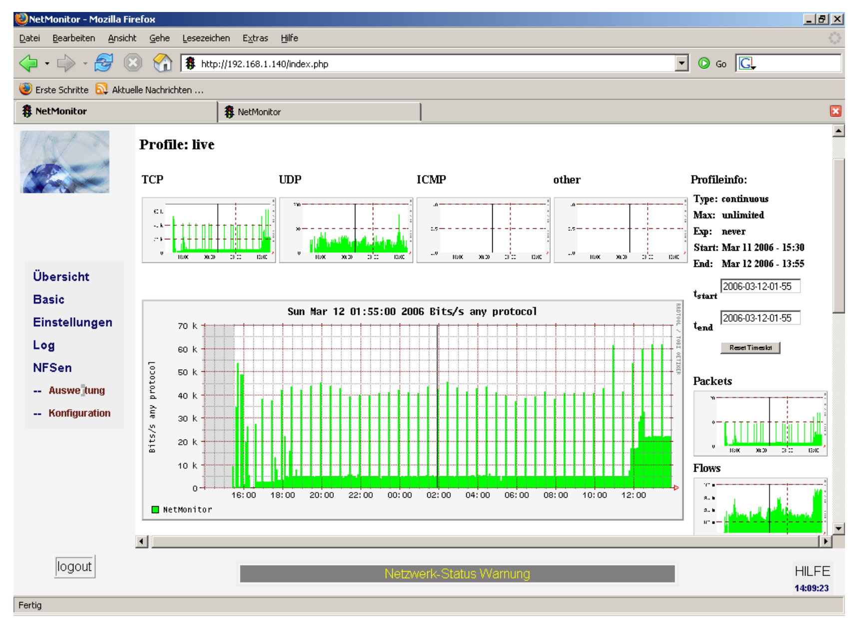


Abbildung 53: NFSen Details Bildschirm

Eine weitere wesentliche Funktion hierbei ist die zeitbezogene Analyse. Im Details Bildschirm wird oben rechts der angezeigte oder analysierbare Zeitraum dargestellt. Im Gegensatz zu herkömmlichen Analysewerkzeugen kann mittels NFSen auch eine Analyse im nachhinein durchgeführt werden.

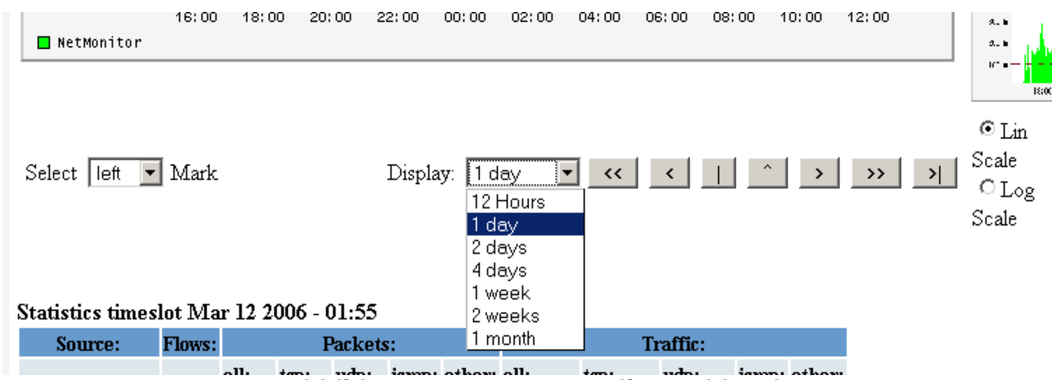


Abbildung 54: NFSen Details Dashbord

Ermöglicht wird dies mit einem Dashbord, welches grundsätzlich auf Zeitbereiche eingestellt werden kann. Auf Basis dieser Auswahl kann mit dem Dashbord rückwärts oder auch vorwärts im Traffic navigiert werden.

Im nachfolgenden Beispiel wurde per Dashbord der Traffic auf den Zeitabschnitt 12.03.06 2.30 Uhr eingestellt. Dies ist mitten in der Nacht von Samstag auf Sonntag und ein Zeitraum, wo sicherlich kein unnötiger Traffic bestehen darf.

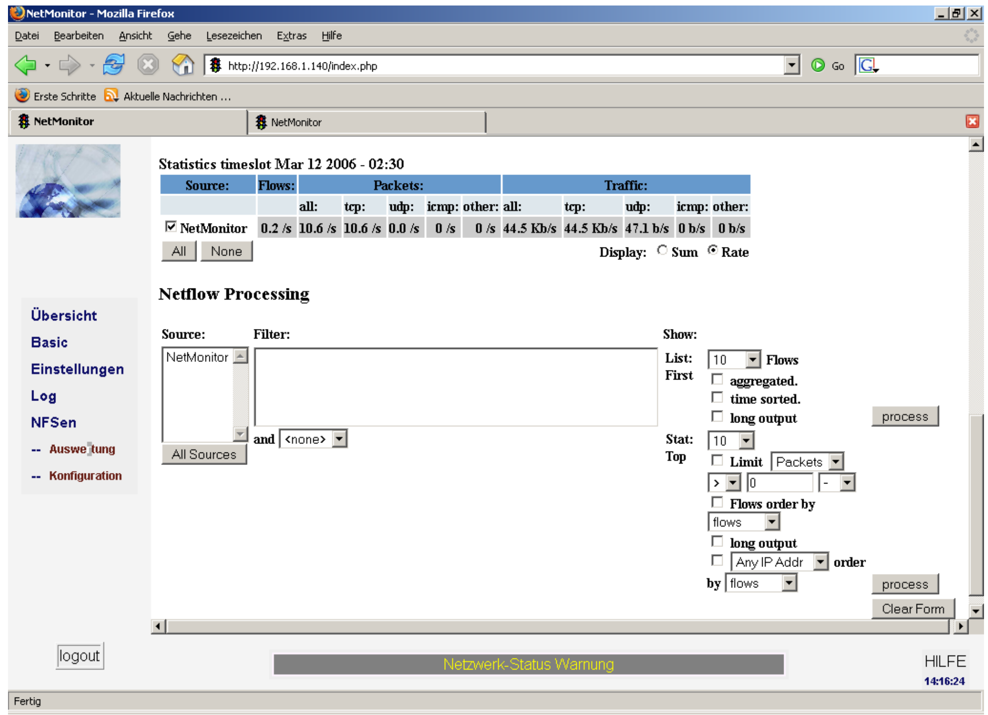


Abbildung 55: NFSen Details Dashbord Zeiteinstellung

Um eine tiefergehende Analyse durchzuführen muss zuerst der Zeitraum eingestellt werden. Dies ist im obigen Beispiel passiert. Im zweiten Schritt wählt man die Probe aus. In diesem Beispiel ist dies der NetMonitor.

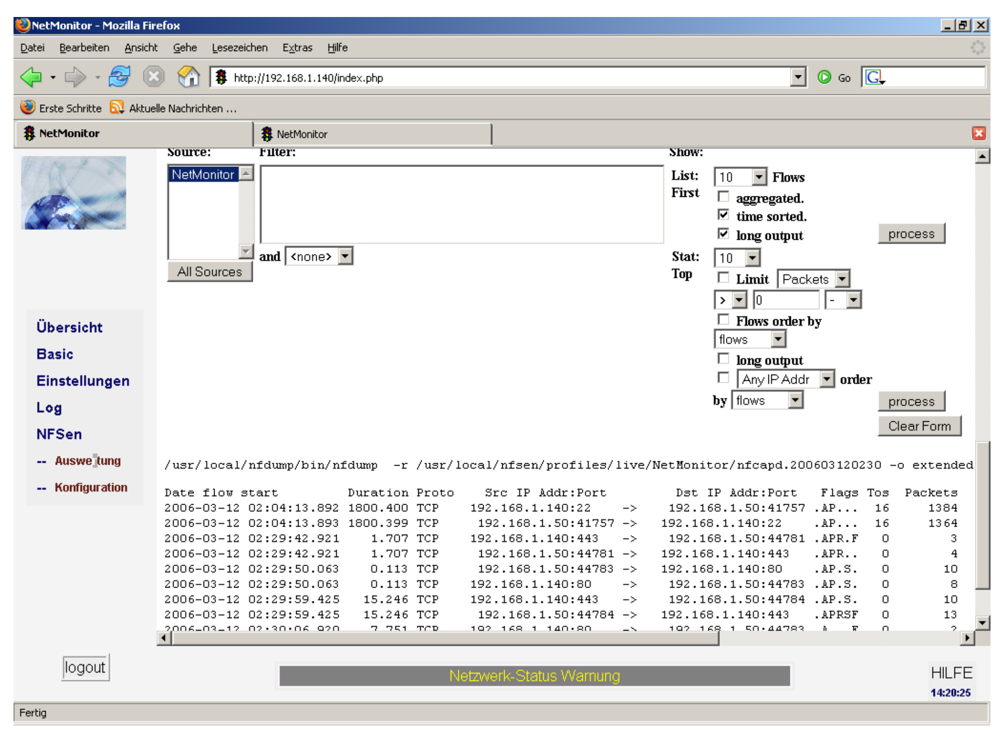


Abbildung 56: NFSen Details Dashbord Analyse

Aus Gründen der Übersichtlichkeit wurde in der obigen Grafik der obere Bereich nicht dargestellt. Wichtig ist in dieser Darstellung die detaillierte Darstellung der Kommunikation zum Zeitpunkt 2.30. Nachfolgend wird dieser Ausschnitt vergrößert dargestellt.

```
/usr/local/nfdump/bin/nfdump  -r /usr/local/nfsen/profiles/live/NetMonitor/nfcapd.200603120230 -o

Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos
2006-03-12 02:04:13.892 1800.400 TCP     192.168.1.140:22      ->    192.168.1.50:41757 .AP...  16
2006-03-12 02:04:13.893 1800.399 TCP      192.168.1.50:41757 ->   192.168.1.140:22      .AP...  16
2006-03-12 02:29:42.921    1.707 TCP     192.168.1.140:443     ->    192.168.1.50:44781 .APR.F   0
2006-03-12 02:29:42.921    1.707 TCP      192.168.1.50:44781 ->   192.168.1.140:443     .APR..   0
2006-03-12 02:29:50.063    0.113 TCP      192.168.1.50:44783 ->   192.168.1.140:80      .AP.S.   0
2006-03-12 02:29:50.063    0.113 TCP     192.168.1.140:80      ->    192.168.1.50:44783 .AP.S.   0
2006-03-12 02:29:59.425   15.246 TCP     192.168.1.140:443     ->    192.168.1.50:44784 .AP.S.   0
2006-03-12 02:29:59.425   15.246 TCP      192.168.1.50:44784 ->   192.168.1.140:443     .APRSF   0
2006-03-12 02:30:06.920    7.751 TCP     192.168.1.140:80      ->    192.168.1.50:44783 .A...F   0
2006-03-12 02:30:06.959    7.712 TCP      192.168.1.50:44783 ->   192.168.1.140:80      .A...F   0
Time window: Mar 12 2006 02:04:13 - Mar 12 2006 02:34:29
```

Abbildung 57: NFSen Details Dashbord Analyse im Detail

Gut zu sehen ist der Zeitframe von 2.04 – 2.34 und die Kommunikation zwischen dem Client 192.168.1.50 auf Port 80 und Port 443 mit dem Server 192.168.1.140.

Auf weitere Details bzw. Möglichkeiten wird an dieser Stelle verzichtet und auf eines der Analyse Seminare verwiesen.

8.2.5 NFSen Auswertung Stats

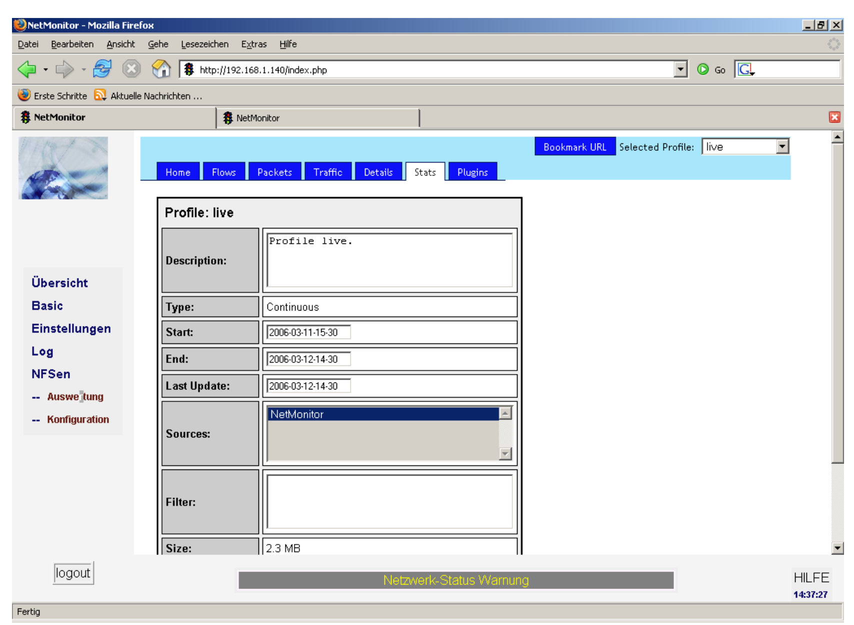


Abbildung 58: NFSen Stats

Im Stats Bildschirm kann man grundsätzliche Attribute, z.B. Beschreibung, Typ des Profil (Profil in diesem Zusammenhang ist eine Auswerteeinstellung), Start- und Endezeitraum des Profils, eventuelle Filter, Datenbankgröße und maximale Datenbankgröße und Veralterungszeitraum einstellen.

8.2.6 NFSen Auswertung Plugins



Abbildung 59: NFSen Plugins

NFSen verfügt über die Möglichkeit weitere Analysen über sogenannte Plugins zu integrieren. Im NetMonitor haben wir ein Plugin (PortTracker) mit integriert, welches die Analyse auf Portebene ermöglicht.

Ähnlich, wie beim Details Bildschirm, wird hier zwischen TCP und UDP, sowie Pakets, Flows und Bytes unterschieden.

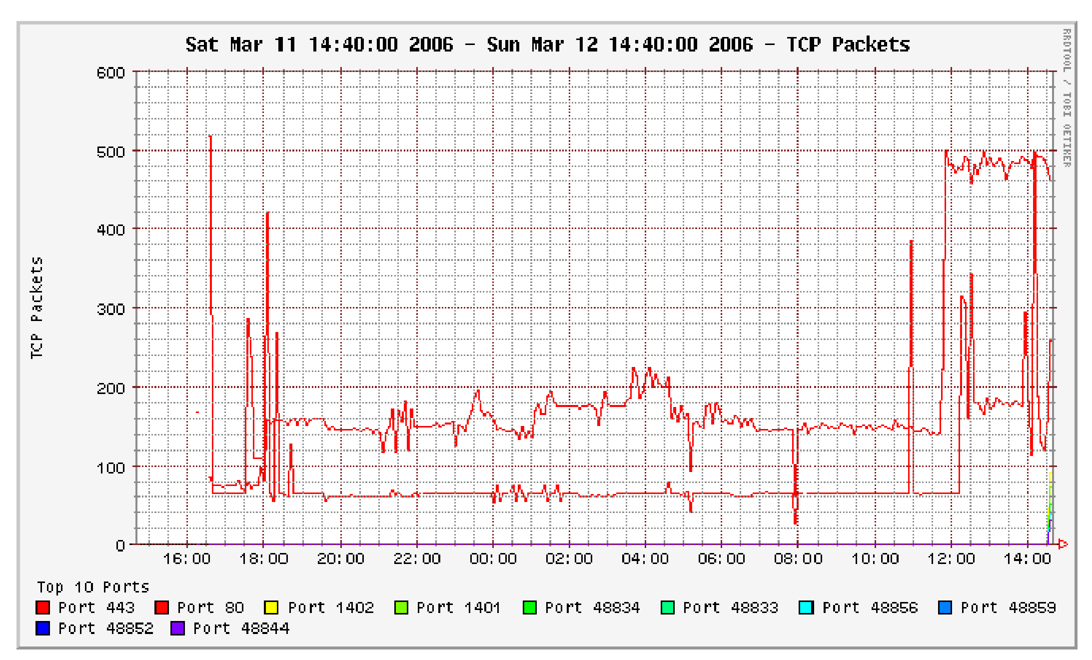


Abbildung 60: NFSen Plugins TCP Packets

Im betrachteten Analysezeitraum wird im obigen Beispiel der traffic anhand der Top 10 Ports dargestellt. Gehen wir wieder auf unser Beispiel mit 2.30 Uhr, so sehen wir hier das ausschließlich der bereits bekannte Traffic vorlag.

Im nachfolgenden Beispiel wurde der Traffic vom Port 443 aus der grafischen Analyse entfernt (skipped ports 443). Über bleibt ausschließlich der Traffic vom Port 80.

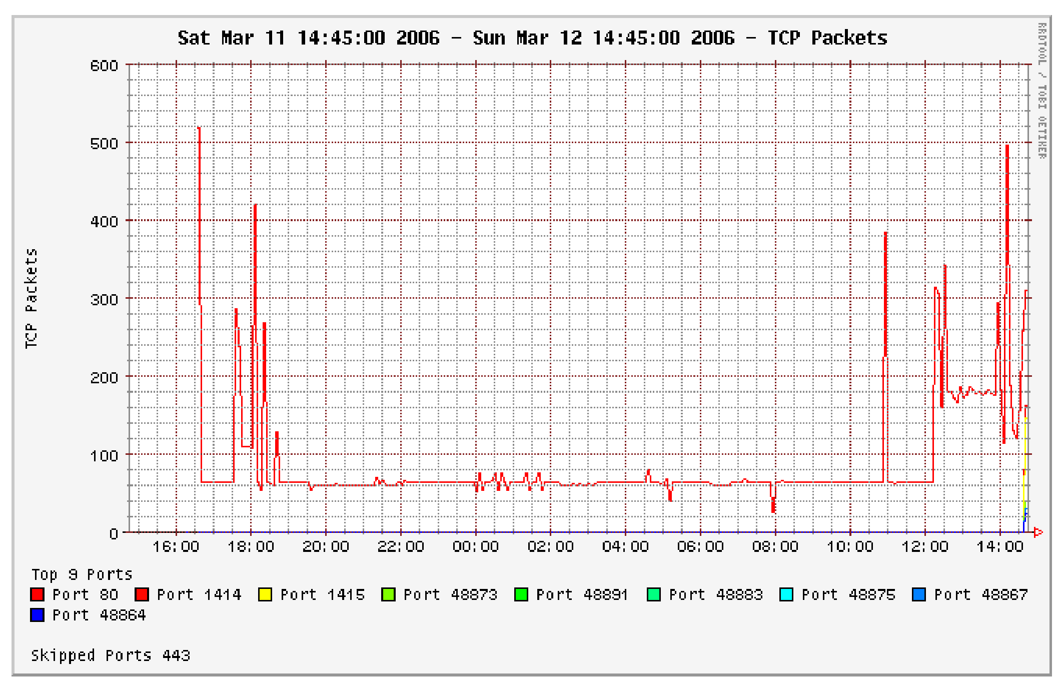


Abbildung 61: NFSen Plugins TCP Packets analysiert

Auf weitere Details bzw. Möglichkeiten wird an dieser Stelle verzichtet und auf eines der Analyse Seminare verwiesen.

8.3 NFSen Konfiguration

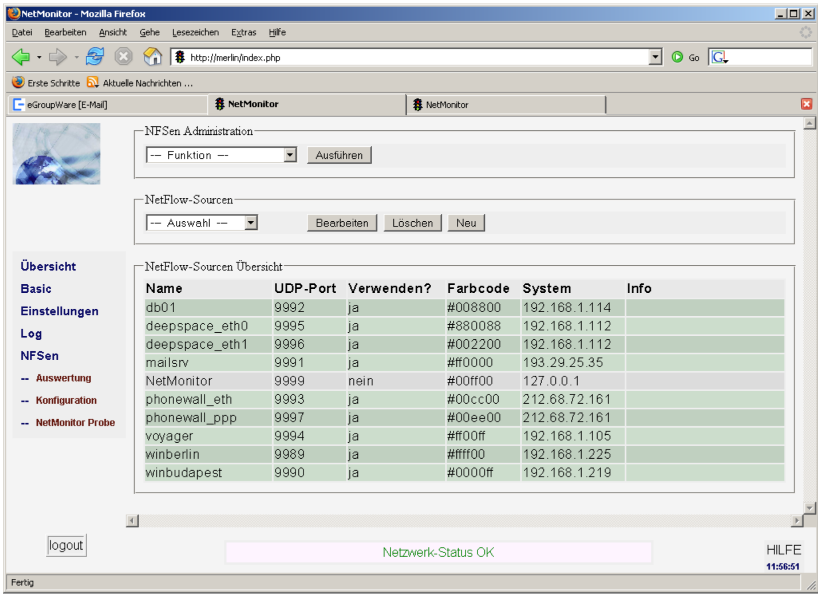


Abbildung 62: NFSen Konfigurationsbildschirm

Der Konfigurationsbildschirm ermöglicht die Administration von NFSen und die Konfiguration von externen Probes.

In der obigen Abbildung ist beides zu sehen.

8.3.1 NFSen Konfiguration Probes

Als erster Schritt ist eine Probe zu konfigurieren. Dies geht über das Dialogfeld „NetFlow Sourcen“.

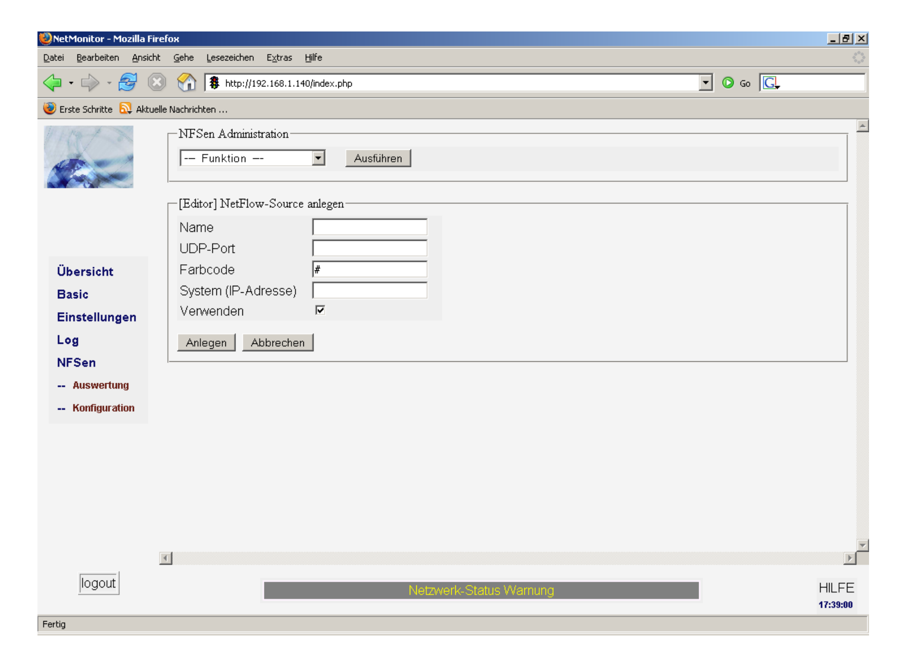


Abbildung 63: NFSen Probe Konfiguration

Über die Auswahl „neu“ wird eine neue Probe ins das System konfiguriert.

- Name
  Der hier konfigurierte Name taucht in den Grafiken als Bezeichnung der Source auf.
- UDP-Port
  Der Port auf dem die Probe die daten (NetFlow Informationen) an den NetMonitor schicken.
- Farbcode
  Mit diesem Farbcode kann jede beliebige Farbe eingestellt werden. Dieser Farbcode bezeichnet in den Grafiken die Sourcen. Nachfolgend einige Beispiele für die Farbcodes:

  ```
  # schwarz     #0f000f   #000f0f   #000000
  # grün        #00ff00   #00f00f   #00cc00
  # dunkelgrün  #008800
  # hellgrün    #00ee00
  # dunkelrot   #e0000f   #c0000f
  # blau        #0000ff
  # rot         #ff0000
  # türkis      #00ffff
  # gelb        #ffff00
  # magenta     #ff00ff
  # weinrot     #880088
  # beige       #cccc00
  ```

- IP-Adresse
  Hier ist die IP-Adresse der Probe anzugeben.
- Info Feld
  ist nicht zur Konfiguration bestimmt (hier werden nur Systennachrichten ausgegeben)

Mit dem Button „Anlegen“ wird die definierte Probe beim NetMonitor in der Datenbank angelegt und steht dann für die weitere Konfigurations-erstellung zur Verfügung.

Mit dem Button „Abbrechen“ wird das Anlegen der Probe in der Datenbank abgebrochen.



Abbildung 64: NFSen Probe Konfiguration Detail

In der Abbildung 57 ist die NetMonitor interne Probe konfiguriert. Dies ist über die IP Adresse 127.0.0.1 zu sehen.

8.3.2 NFSen Konfigurations Erstellung

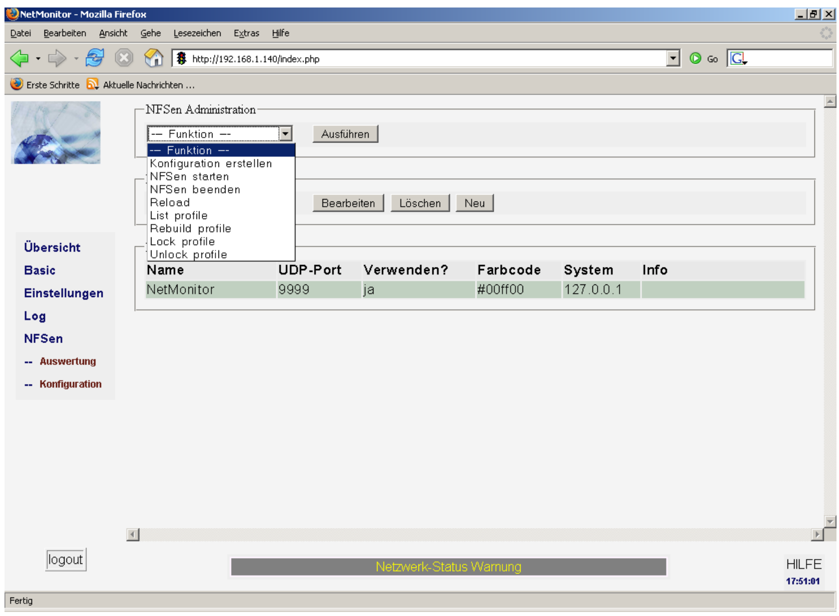


Abbildung 65: NFSen Konfigurationserstellung

Die obige Abbildung zeigt den Bildschirm mit dem die Konfiguration für NFSen erstellt wird. Die nachfolgende Abbildung zeigt in einer Detaildarstellung die weiteren Möglichkeiten der Administration von NFSen.

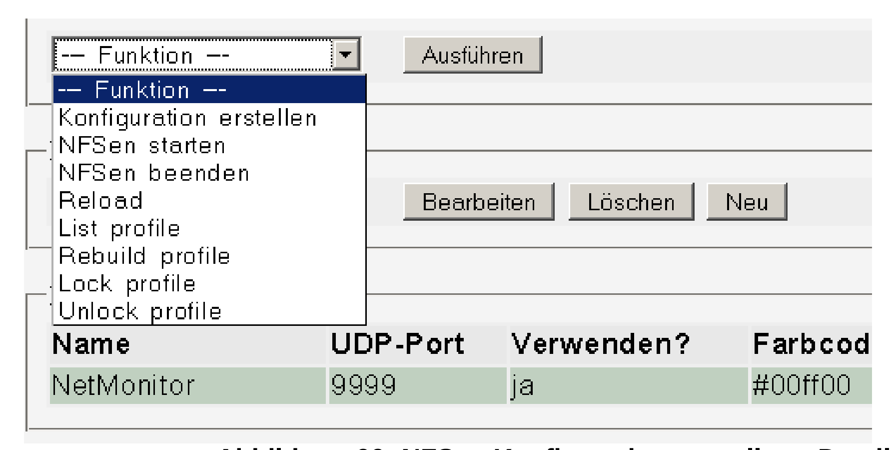


Abbildung 66: NFSen Konfigurationserstellung Detail

Für die Konfigurationserstellen ist ausschließlich die oberste Funktion im obigen Dialog zuständig. Alle weiteren Funktion betreffen die Administration von NFSen.

Die Konfiguration wird erstellt indem zuerst die Probes aus der datenbank ausgewählt werden und falls diese dann für den Betrieb genutzt werden sollen, wird die Konfiguration erstellt.

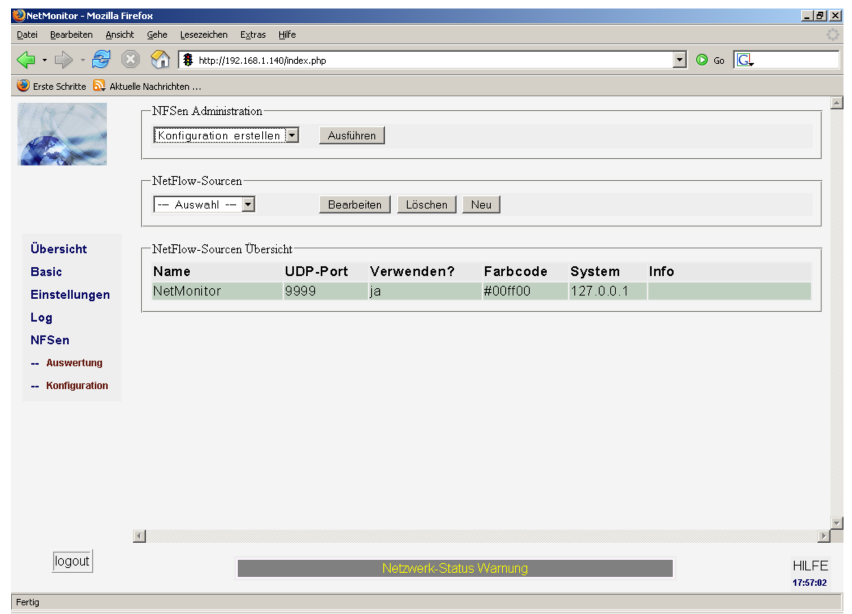


Abbildung 67: NFSen Konfigurationserstellung Schritt 1

Schritt 1 der Konfigurationserstellung ist die Auswahl des Dialogs und die Bestätigung mit dem Klick auf den Button „Ausführen".

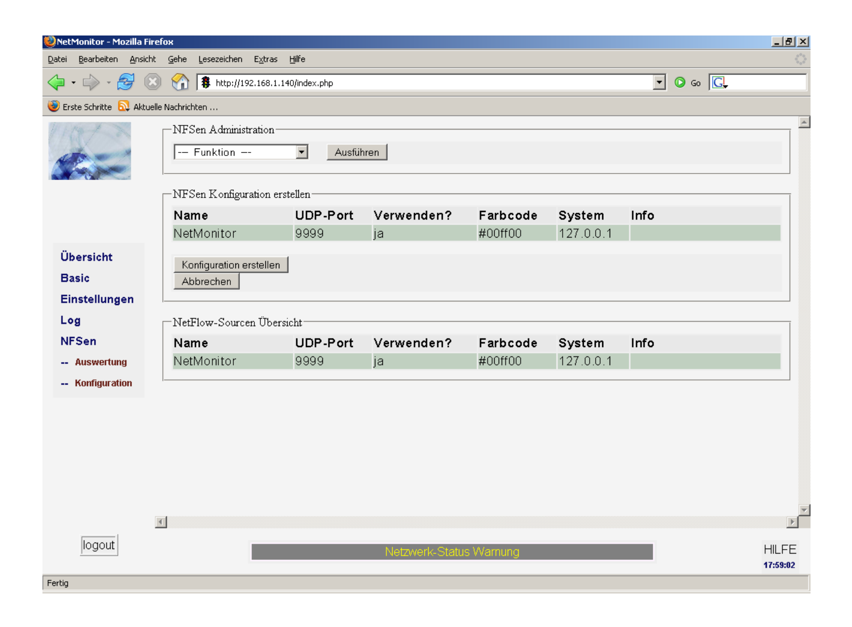


Abbildung 68: NFSen Konfigurationserstellung Schritt 2

Als Ergebnis kommt eine tabellarische Darstellung der aktuellen Konfiguration. Hier kann die künftige Konfiguration noch mal bewertet werden. Mit Klick auf den Button „Konfiguration erstellen“, wird die neue Konfiguration erstellt.

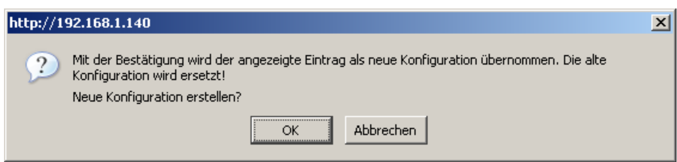


Abbildung 69: NFSen Bestätigung Konfigurationserstellung

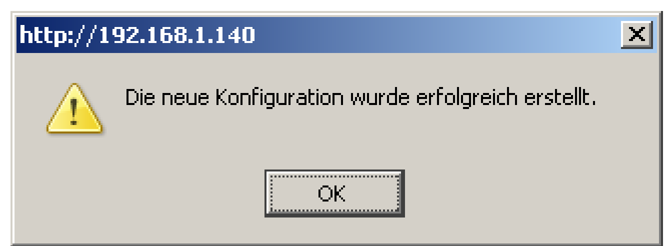


Abbildung 70: NFSen Bestätigung der Konfiguration

Hiermit ist die Erstellung der neuen Konfiguration abgeschlossen.

8.3.3 NFSen Administration

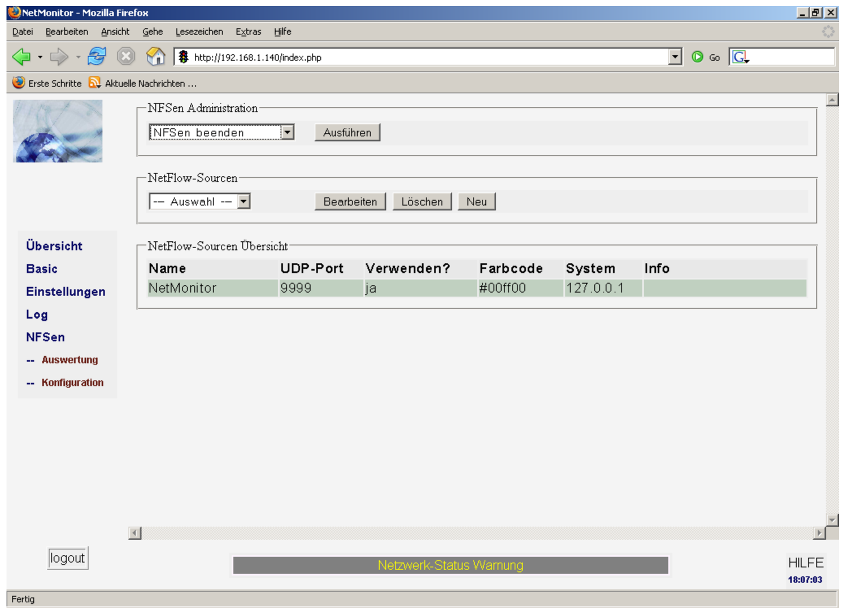


Abbildung 71: NFSen Beenden

Über den Button „NFSen beenden“ wird NFSen beendet. Dies kann je nach Laufzeit der Umgebung bis zu 2 Minuten dauern.

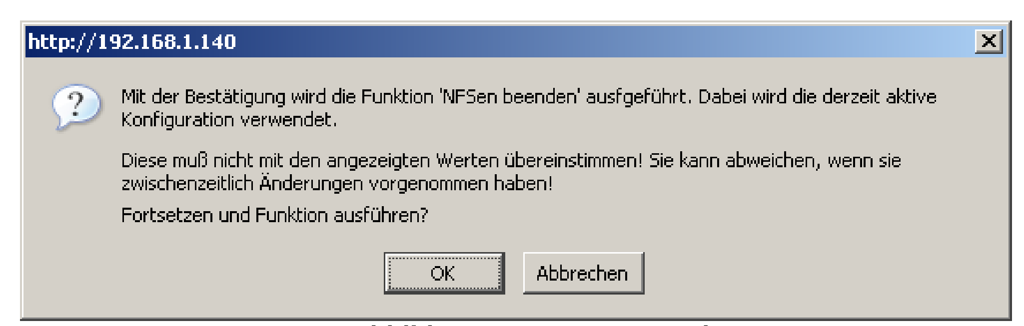


Abbildung 72: NFSen Beenden

Bestätigungsdialog beim Beenden von NFSen.

Mit der Bestätigung wird NFSen deaktiviert und alle Prozesse werden herunter gefahren.

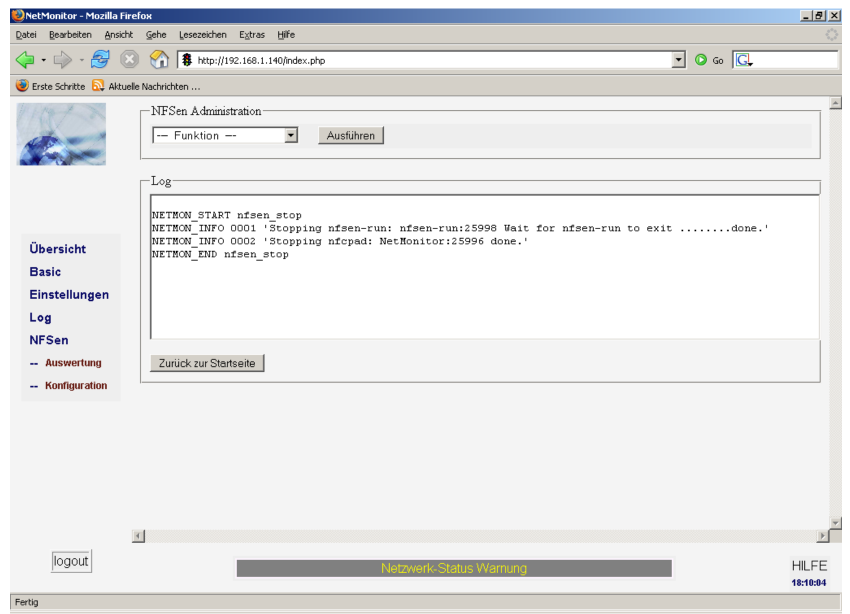


Abbildung 73: NFSen Beenden „Information“

Über den obigen Dialog können Sie sehen, das NFSen ordnungsgemäß beendet wurde.

Mit dem Klick auf den Button „Zurück zur Startseite“ gelangen Sie wieder auf den Konfigurationsbildschirm.

- NFSen Starten
  Hierüber wird NFSen gestartet
- NFSen Beenden
  Siehe obige Beschreibung
- Reload
  Falls Änderungen am Profil durchgeführt worden, muss ein Reload von NFSen durchgeführt werden
- List Profile
  Darstellung des aktuellen Profils
- Rebuild Profile
  Falls im Profil Fehler entstanden sind, muss ein Rebuild durchgeführt werden
- Lock profile
  Falls Änderungen am Profil verhindert werden sollen, kann es hierüber “verschlossen” werden
- Unlock Profile
  Falls das profil aufgrund von Änderungen “verschlossen” wurde, kann es hierüber frei gemacht werden

8.4 NFSen NetMonitor Probe

Wie aus den vorhergehenden Kapiteln bereits deutlich wurde, wird für die Nutzung von NFSen beim NetMonitor mindestens eine Probe benötigt.

In vielen Fällen reicht es aus, für eine tiefergehende Analyse mit einer Fast Ethernet Probe zu arbeiten. Diese Funktion wurde beim NetMonitor mit integriert.

Der NetMonitor wird standardmäßig mit zwei Fast Ethernet Schnittstellen ausgeliefert. Die Schnittstelle eth0 (von vorn betrachtet ganz rechts unten) ist für die normale Kommunikation und das Monitoring vorgesehen. Die Schnittstelle eth1 (von vorn betrachtet ganz rechts oben) kann für die Fast Ethernet Probe genutzt werden.

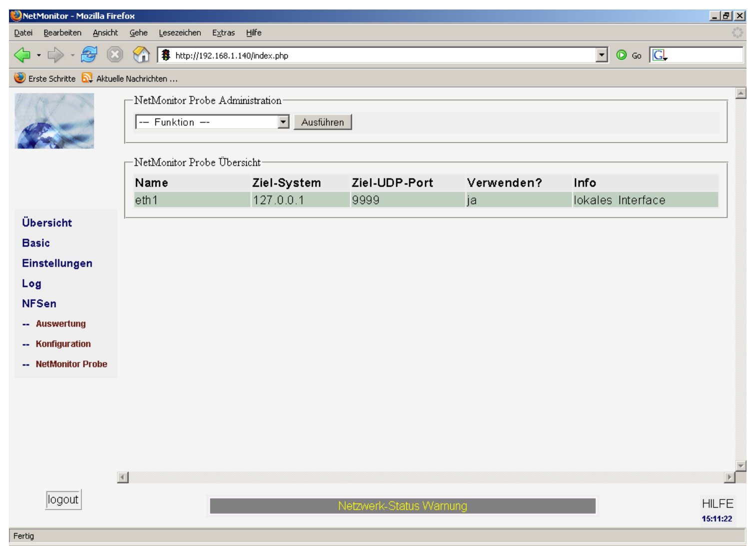


Abbildung 74: NFSen NetMonitor Probe

Die Konfiguration der eingebauten Probe ist fest erstellt und kann nur aktiviert oder deaktiviert werden.

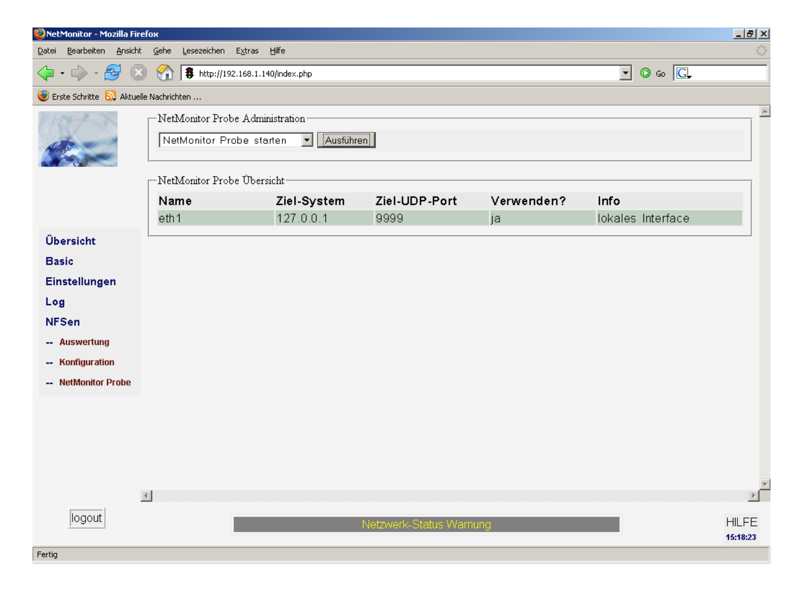


Abbildung 75: NFSen NetMonitor Probe starten

Der Startvorgang ist in Abbildung 67 gesehen werden. Nach dem Starten der NetMonitor Probe kommt noch die nachfolgende Sicherheitsabfrage.



Abbildung 76: NFSen NetMonitor Probe starten Sicherheitsabfrage

Mit Bestätigung der Sicherheitsabfrage wird die interne NetMonitor Probe gestartet und kann dann, wie bereits beschrieben, in NFSen mit in die Konfiguration genommen werden.

8.5 NFSen betreiben

NFSen ist, wie bereits mehrfach gesagt, eine Software mit der das NetFlow Protokoll gelesen und die entsprechenden Informationen analysiert werden können.

NetFlow hat anders als andere Analyse Werkzeuge die Möglichkeit rückwärts den Traffic zu analysieren. Um dieses zu unterstützen sind Datenbanken notwendig in denen die entsprechenden Informationen gespeichert werden. Alle Informationen werden dann zur Laufzeit aus den Datenbanken gelesen und ausgewertet.

Die beim NetMonitor durchgeführte Implementierung ermöglicht auch eine Server spezifische Auswertung des jeweiligen Traffics. Hierzu ist es zum einen notwendig für diesen Server eine entsprechende Probe zu installieren und zum zweiten muss ein entsprechendes Profil angelegt werden.

Nachfolgend gehen wir auf diese Zusammenhänge ein und erklären, wie mit einfachen Schritten eine zufriedenstellende Grundkonfiguration erreicht wird.

8.5.1 NFSen Probes betreiben

Um ein Server spezifisches Profil zu erhalten, ist es notwendig sich nur den Traffic eines einzelnen Servers anzusehen. Dies kann über Filterlisten mit entsprechenden Werkzeugen, aber auch über den NetMonitor geschehen.

Es bestehen zwei grundsätzliche Möglichkeiten beim NetMonitor:

- Nutzung einer externen Probe, z.B. NF-Probe von Nomics

- Nutzung einer internen Probe, z.B. NF-UX oder NF-Win von Nomics

Auf die Konfiguration der Probes wird hier nicht weiter eingegangen, da dies in den jeweiligen Handbüchern beschrieben ist.

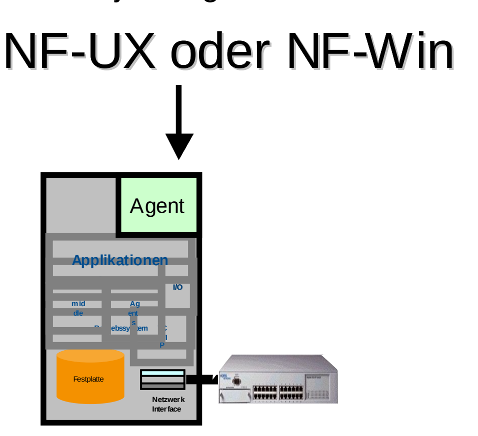


Abbildung 77: interne Probe auf einem Server

Die obige Abbildung zeigt den Einsatz einer internen Probe. Wird diese Probe ausschließlich auf das Serverinterface konfiguriert, so erhält man über diese Server spezifische Source ein Server spezifisches Trafficverhalten. Wird diese verhalten über einen längeren zeitraum beobachtet, bzw. aufgezeichnet, so kann man sehr schnell Abweichungen und Unregelmäßigkeiten identifizieren.

Nachfolgend muss diese Server Probe, wie bereits beschrieben, im NFSen erstellt und mit in die NFSen Konfiguration übernommen werden. Näheres hierzu in den jeweiligen Kapitel des vorliegenden Benutzerhandbuchs.

Bei dem Einsatz einer externen Probe ist im Prinzip ähnlich vorzugehen.

Zuerst muss bei einem entsprechenden Layer 2 oder Layer 3 Switch ein Port Mirror eingerichtet werden. Danach muss die Probe installiert und konfiguriert werden. Im letzten Schritt muss auch diese externe Probe, wie bereits beschrieben, im NFSen erstellt und mit in die NFSen Konfiguration übernommen werden.

Für jede interne oder externe Probe muss ein Eintrag in der NFSen Konfiguration bestehen. Falls dies nicht der Fall ist, werden die Daten dieser Probe nicht ausgewertet und stehen für eine Analyse nicht zur Verfügung.

Eine Serverprofil ist aus wirtschaftlichen Gesichtspunkten meistens nur mit einer internen Probe zu realisieren. Auf einer externen Probe werden im Regelfall verschiedenen Datenströme zusammen gefasst. Bei der NF-Probe von Nomics ist es jedoch möglich je Interface eine Probe zu realisieren. Damit stellt die NF-Probe von Nomics in einem Gehäuse bis zu vier parallele Probes zur Verfügung mit denen dann zum einen der

Netzwerktraffic aber auch spezifischer Servertraffic analysiert werden kann.

8.5.2 NFSen Profile betreiben

Sinnvollerweise wird für jede Serverprobe ein eigenständiges Profil angelegt.

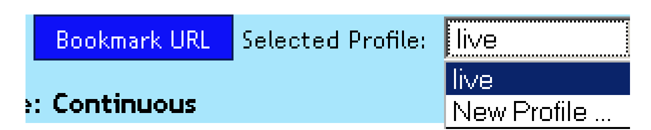


Abbildung 78: Erstellen eines Serverprofils

Der Ausschnitt in der obigen Abbildung zeigt das aktuelle Profil „live“ an. Darunter kann man ein neues Profil anlegen.

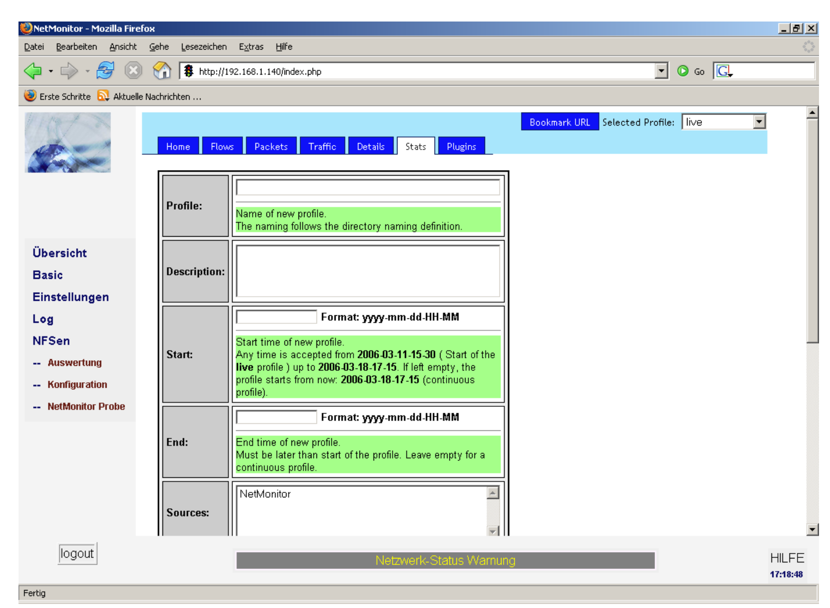


Abbildung 79: Konfiguration eines Serverprofils

Zuerst gibt man einen Namen für das neue Profil an und erstellt eine sinnvolle Beschreibung. Weiter kann definiert werden, in welchen Zeiträumen das Profil gültig ist und welche Probe zu dem Profil gehört.

Falls man kein Serverprofil anlegen möchte, sondern ein Netzsegment spezifisches profil, so kann man hier mehr als eine Probe (je nach Möglichkeiten) einrichten.

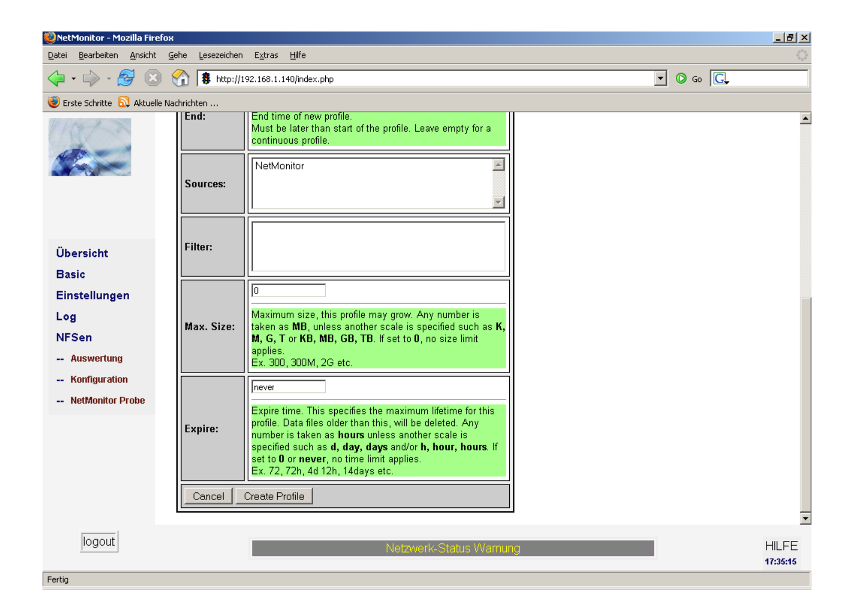


Abbildung 80: Konfiguration eines Serverprofils

Falls in dem Profil nur spezieller Traffic, z.B. Datenbank Traffic betrachtet werden soll, so kann dies über einen entsprechenden Filter realisiert werden. Die Regeln für diesen Filter sind TCPDUMP kompatibel.

Zum Schluss kann die maximale Größe des Profils eingestellt werden und wann die Daten veraltern.

Wichtig!! Läuft ein Profil mit vielen Probes über einen langen Zeitraum, so können hier schnell Dateigrößen oberhalb von 2 Gbyte entstehen. Es ist also wichtig die Betriebssystemeigenschaften an der Stelle zu kennen. Beim NetMonitor sind Dateigrößen bis zu 4 Gbyte möglich. Falls mehr benötigt werden sollte, so ist beim Service hierzu anzufragen.

8.5.3 NFSen Datenbanken betreiben

Die Daten, welche durch ein Profil beschrieben werden, werden in Datenbanken gespeichert. Abhängig von der Analyse kommen unterschiedliche Datenbanken zum Einsatz. Die Summe der Datenbanken liegt bei ca. 10 Gbyte im Minimum und kann in einem längeren Zeitraum das gesamte Dateisystems des NetMonitor auffüllen.

Aus den obigen Darstellungen wird klar, das, wenn eine Rückwärtige Analyse des Traffics in den beschrieben Datenbaken durchgeführt werden soll, zumal es mehrere (ca. 70 unterschiedliche) sind, es auf eine hohe Synchronisation der Datenbanken ankommt.

Wird NFSen gestartet und kontinuierlich betrieben, so wird die Synchronisation kontinuierlich durchgeführt. Dies geschieht mit Hilfe von speziellen Zeitstempeln.

Wird NFSen über einen längeren Zeitraum, z.B. einige Tage nicht betrieben und soll wieder in Betrieb genommen werden, so wird automatisch eine Synchronisation der Datenbanken durchgeführt. Da NFSen nicht wissen kann, ob der bereits in den Datenbanken gespeicherte Traffic relevant ist oder nicht, wird die Synchronisation über alle Datenbanken durchgeführt. Dies führt bei einer grösseren Datenbank zu einer enormen CPU- und Speicherauslastung. Schlimmsten falls kann das gesamte System davon betroffen sein da alle Ressourcen für die Synchronisation genutzt werden.

Aus der Erfahrung hat sich gezeigt, das es im Regelfall nicht notwenig ist die Synchronisation während des Betriebs durchzuführen, sondern eine Datenbank Initialisierung vor der neuen Inbetriebnahme ausreicht.

Die Datenbank Initialisierung ist bereits bei der Administration beschrieben worden und wird hier nicht weiter erklärt. S sei nur darauf hingewiesen, das die Datenbank Initialisierung ca. 30 Minuten benötigt und man in dieser Zeit in Ruhe einen Kaffe trinken kann.

8.5.4 NFSen Administration durchführen

Aus dem vorherigen Abschnitt ist deutlich geworden, das es Sinn macht beim Betrieb von NFSen eine gewisse Arbeitsschrittreihenfolge einzuhalten.

Nachfolgend werden die Arbeitsschritte bzw. Die Reichenfolge der Administrationskommandos für NFSen beschrieben.

8.5.4.1 NFSen Arbeitsschritte “NFSen starten”

Die Arbeitsschritte für die Erstinbetriebnahme von NFSen ist folgende:

1. Probe einrichten (Installation eines externen Probe oder Installieren einer internen Probe)
2. Probe im NFSen konfigurieren und NFSen Konfiguration entsprechend einstellen
3. Datenbank Initialisierung durchführen
4. NFSen starten

8.5.4.2 NFSen Arbeitsschritte “Profil erstellen”

Die Arbeitsschritte für die Erstellung eines Profils ist folgende:

1. NFSen stoppen

2. Probe einrichten (Installation eines externen Probe oder Installieren einer internen Probe)
3. Probe im NFSen konfigurieren und NFSen Konfiguration entsprechend einstellen
4. Profil einstellen
5. NFSen starten

8.5.4.3 NFSen Arbeitsschritte “Profil warten”

Die Arbeitsschritte für die Erstellung eines Profils ist folgende:

1. NFSen stoppen
2. Rebuild des Profils
3. NFSen starten

8.5.4.4 NFSen Arbeitsschritte “Profil Datenbank warten”

Die Arbeitsschritte für die Erstellung eines Profils ist folgende:

1. NFSen stoppen
2. Rebuild des Profils
3. NFSen starten
4. Profil anzeigen (listen)
5. falls Profil gesperrt ist (locked = 1)
6. Profil entsperren (unlock)
7. NFSen reload durchführen

Falls trotz der obigen Maßnahmen die Datenbank nicht synchronisiert werden kann, so ist NFSen zu stoppen und eine Datenbank Initialisierung durchzuführen.

8.5.4.5 NFSen Arbeitsschritte “NFSen Wiederinbetriebnahme”

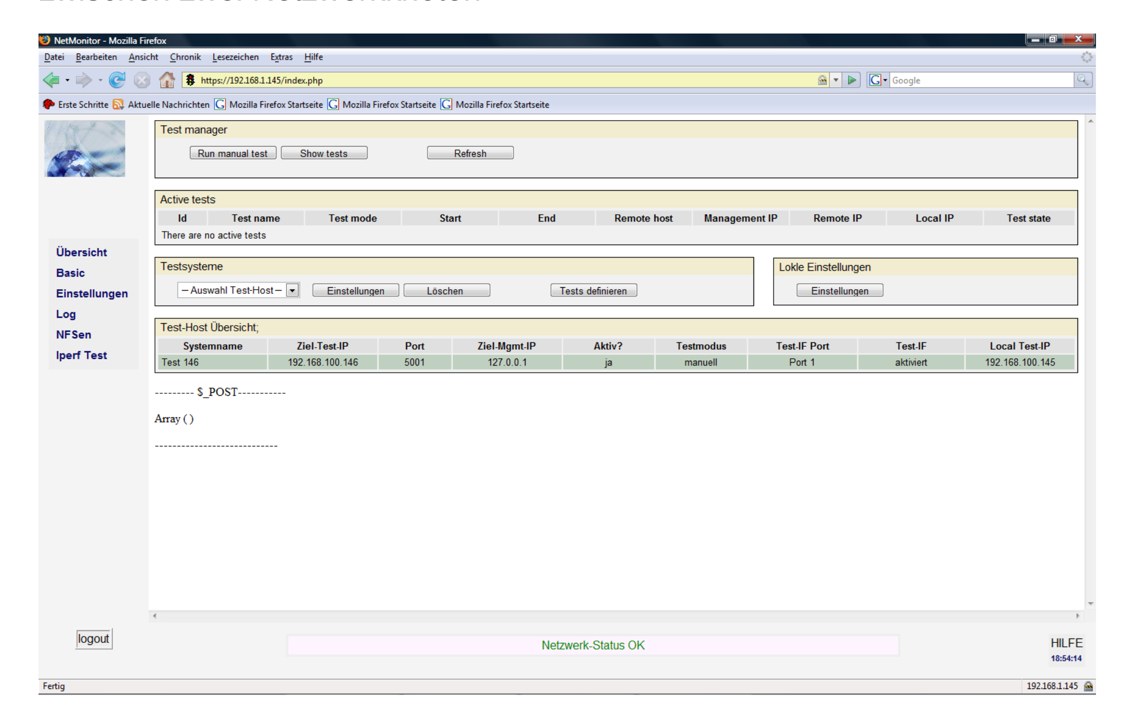
Die Arbeitsschritte für die Wiederinbetriebnahme von NFSen ist folgende:

1. Probe einrichten (Installation eines externen Probe oder Installieren einer internen Probe)

2. Probe im NFSen konfigurieren und NFSen Konfiguration entsprechend einstellen
3. Datenbank Initialisierung durchführen
4. NFSen starten
5. Profile anpassen, bzw. Warten
6. NFSen reload durchführen

9 Iperf Test

Iperf ist Open Source und misst den maximalen Datendurchsatz via TCP, zwischen zwei Netzwerkknoten.



Standard Bildschirm von Iperf

Mit Iperf lässt sich, via TCP, der Datendurchsatz zwischen zwei Netzwerkknoten messen. Dabei dient einer als Server und ein zweiter als Client.

Iperf ermöglicht:

- Messen eines TCP Streams zwischen zwei Netzknoten
- Einfaches navigieren zwischen den einzelnen Messungen
- Auswerten der einzelnen Daten der Bandbreiten Messung
- Einfache Anpassung an das jeweiligen Netzwerk

9.1 Interfaces

Mit Aufrufen der Lokalen Einstellungen gelagt man in den Bilschirm, wo man die Interfaces festlegen kann.

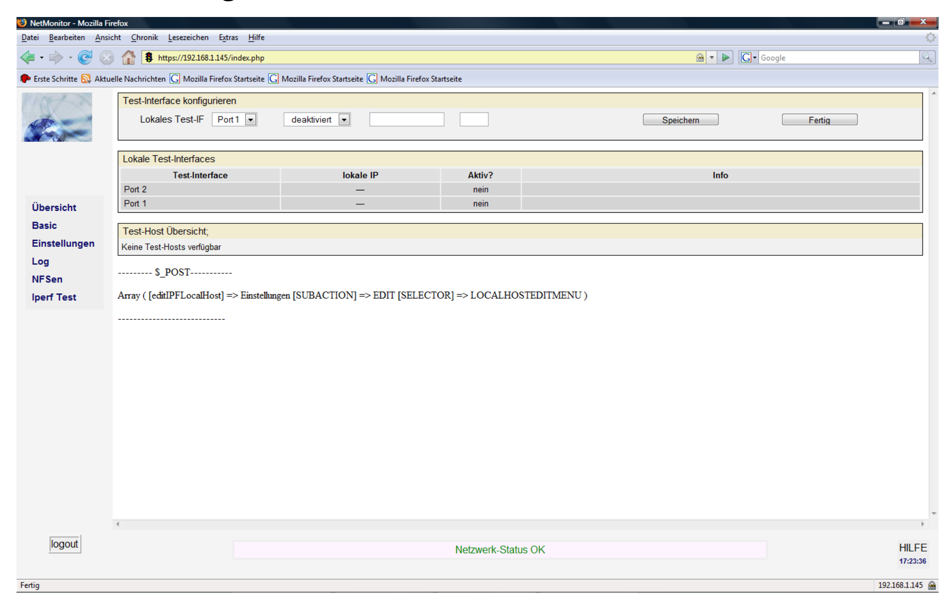


Abbildung 82: Interface konfigurieren

Über den Menüpunkt Lokales Test IF, werden die einzelnen Interfaces Konfiguriert. Anhand des Puldown Menüs, kann man das Interface auswählen. Im zweiten Puldown Menü wird der Status, auf aktiviert oder deaktiviert gestellt. In der Regel sollte der Status auf aktiviert gestellt werden. Bevor in den beiden dahinter liegenden Feldern die IP Adresse und das Subnetz eingetragen werden, von wo aus der TCP Stream losgeschickt werden soll. Zum Schluss muss die Konfiguration nur noch, mit der Schaltfläche Speicher bestätigt werden.

Ist die Konfiguration des Interfaces unvollständig, wird man über eine Fehlermeldung darüber Informiert welche Einstellungen nicht korrekt sind.

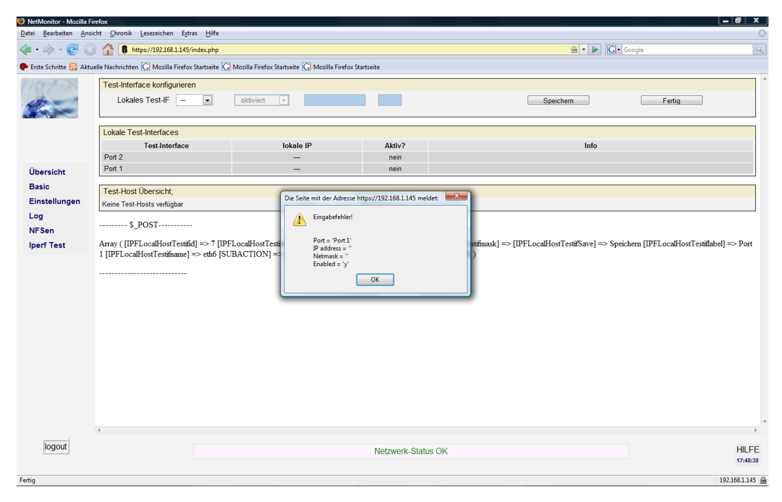


Abbildung 82: Fehlermeldung unvollständige Eingabe

Es wird, in der Regel nur ein Lokales Interface benötigt, dass zweite kann man also frei lassen.
Ist das, mit Port 1 bezeichnete Interfaces konfiguriert, kommt man durch bestätigen der Schaltfläche Fertig, zum ausgangs Bildschirm zurück.

9.2 Test Host

Im nächsten Schritt, wird ein Test Host benötigt. Dieser wird, durch betätigen der Schaltfläche Neu, in der Spalte Testsysteme erstellt.

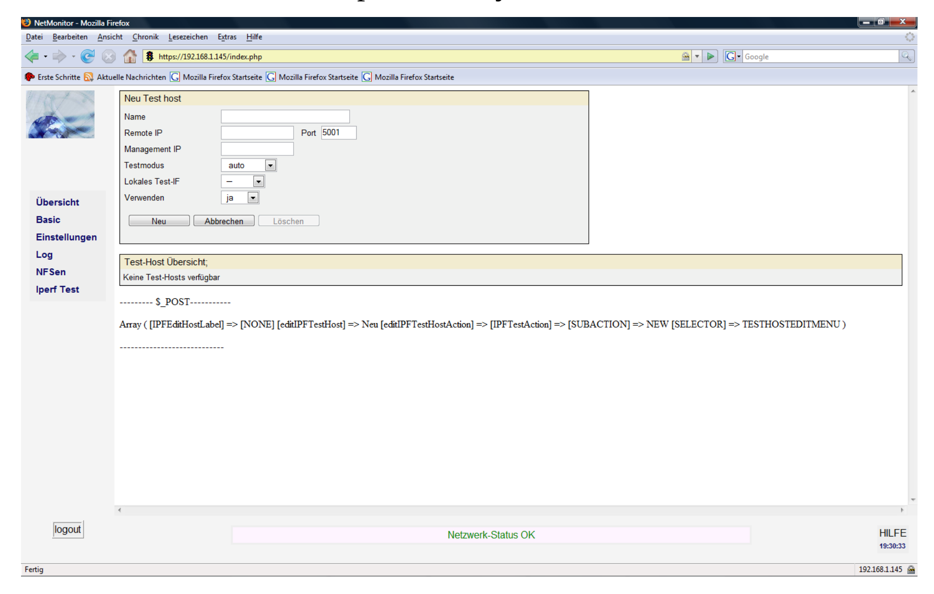


Abbildung 83: Test Host erstellen

Hierbei ist, darauf zu achten, dass alle Felder ausgefüllt werden, ansonsten erscheit wie schon in Abbildung 82 zu sehen, eine Fehlermeldung.

Zur Erläuterung der Werte:

- Name = ein beliebiger Name für den Test Host
- Remote IP = Ip – Adresse, des Remote Systems
- Management IP = Management Ip – Adresse, des Remote Systems
- Testmodus = Ob der Test Automatisch oder Manuell durgeführt werden soll
- Lokales Test IF = auf welchen Port das Lokale Test Interface liegt
- Verwenden = ob der Test Host sofort Verwendet werden soll, oder später

Wenn die oben beschriebenen Felder sorgfältig ausgefüllt und vervollständigt worden sind, kann dieser Prozess, mit Neu bestätigt werden.

9.3 Test definieren

Um einen Test zu definieren, muss als erstes, auf der Startseite von Iperf Test, das zu verwendende Testsystem ausgewählt werden. Ist das Testsystem, in der Spalte Testsysteme ausgewählt, bestätigt man dieses mit Tests definieren. Im anschluss, erscheint volgender Bildschirm

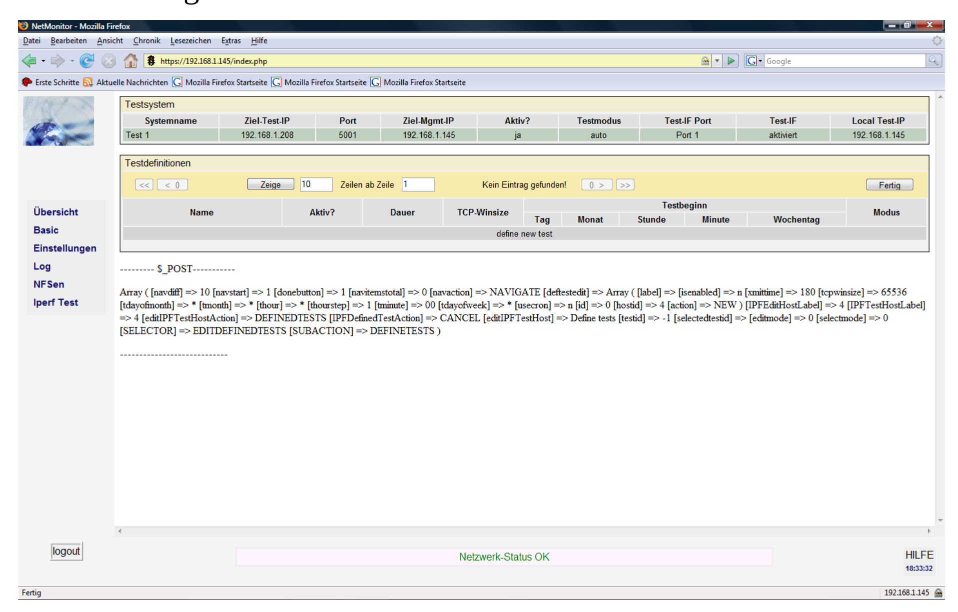


Abbildung 84: Test definieren

In der oben gezeigten Abbildung, sieht man im oberen Bereich, dass ausgewählte Testsystem und im darunter liegenden Bereich, die Testdefinitionen.
Um einen Test zu definieren, wird wie folgt vorgegangen:

- anklicken der Schrift „define new test“
- ergänzen der nun Angezeigten Felder
  - Name = beliebiger, aber eindeutiger Name, des Test´s
  - Aktiv = ob der Test Aktiviert werden soll oder noch nicht
  - Dauer = Hier kann die Dauer der Zeit eingestellt werden, wie lange der Test, in einer Richtung laufen soll. Zur Info, wenn z.B 180 eingestellt wird, benötigt der Test 2 x 180 Sekunden, da der TCP Stream in beiden Richtungen erfolgt.
  - TCP-Winsize = unter diesem Punkt, kann der TCP Stream eingestellt werden
  - Tag = an welchem Tag, der Test laufen soll, bei Stern Täglich
  - Monat = in welchem Monat der Test laufen soll, bei Stern

Monatlich

- o Stunde/Minute = zur welcher Uhrzeit der Test laufen soll, bei Stunde kann ein Stern für Stündlich eingesetzt werden, bei Minute muss eine Zahl eingetragen werden.
- o Wochentag = an welchem Wochentag der Test laufen soll, bei Stern Wöchentlich.
- o Modus = ob der Test manuell oder automatisch gestartet werden soll. Wobei, wenn hier automatisch eingestellt wird, darauf zu achten ist, das in der Konfiguration des Test Interfaces, auch automatisch stehen muss.

Diese Werte, können in verschiedenen Warianten, vorgenommen werden. Je nachdem, wie groß die Packte sein sollen, die durch die Leitung geschickt werden und zu welcher Zeit, der Test durchlaufen soll. Der Iperf Test, kann auch mit der oben genannten Einstellung Automatisiert werden, so dass dieser z.B einmal Wöchentlich oder, einmal pro Tag durchgeführt wird.

Sind die Einstellungen wunschgemäß vorgenommen worden, brauch man diese nur noch mit speichern bestätigen und im Nachfolgenden Fenster, auf Fertig klicken.

9.4 Test manuell starten

Es kann auch, ein bereits definierter Test manuell gestartet werden. Hierzu geht man, auf die Startseite von Iperf Test und wählt im oberen bereich, unter Test-Manager, den Button Manueller Test.

Im Anschluß erscheint folgende Darstellung.

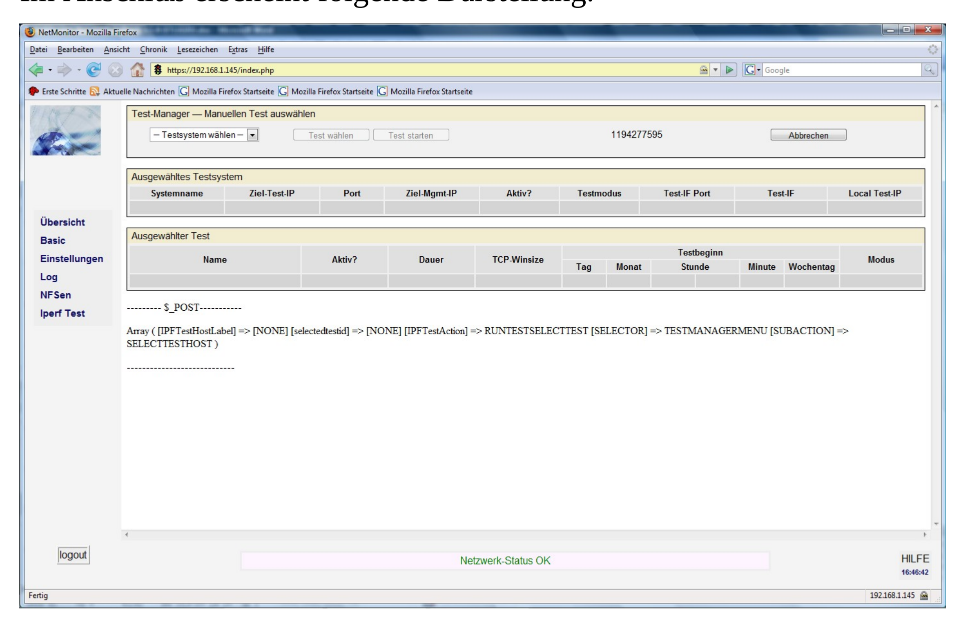


Abbildung 84: Manueller Test

Als erstes, wird im oberen Bereich, unter Test-Manager, das Testsystem ausgewählt. Wird das Testsystem, im mittleren Bereich angezeigt, werden im darunter liegendem Bereich, die dem Testsystem zugeordneten Test´s aufgelistet. Hier wird der Test, den man verwenden möchte, durch einen klick mit der Maus bestätigt. Im nachfolgenden Fenster erscheint, der Test, dann in der Spalte Ausgewählter Test. Im nächsten Schritt, braucht man, den Test nur noch über den Button Test starten bestätigen.
Wichtig hierbei ist, um einen Test durchzuführen, muss das Remote System, auch online sein und dementsprechend Konfiguriert sein. Vor allem müssen, die Werte der IP- Adressen stimmen, die zuvor bei der Definition des Testsystems vorgenommen worden sind.

9.5 Testergebnisse anzeigen

Um sich die Testergebnisse anzeigen zu lassen, geht man auf der Startseite von Iperf Test, im oberen Bereich auf den Button Testergebnisse. Nadem die neue Seite geladen ist, muss als nächstes ein Filter gesetzt werden, damit Test ergebnisse angezeigt werden. Standart messig, steht in dem dafür vorgesehenden Drop Down Feld "Aktive Tests", somit würden auch nur die momentan Laufenden Tests angezeigt. Wenn man hier also das Drop Down Feld benutzt, bekommt man volgende auswahl möglichkeiten.

- Aktive Tests
- Neue Testergebnisse
- Neue erfogreiche Tests
- Neue fehlgeschlagende Tests
- Alte erfogreiche Tests
- Alte felgeschlagende Tests
- Alle erfogreichen Tests
- Alle fehlgeschlagenden Tests
- Alle Tests

Ist ein Filter gesetzt, wird im darunter liegenden Bereich, die dem Filter zugeodneten Tests angezeigt.

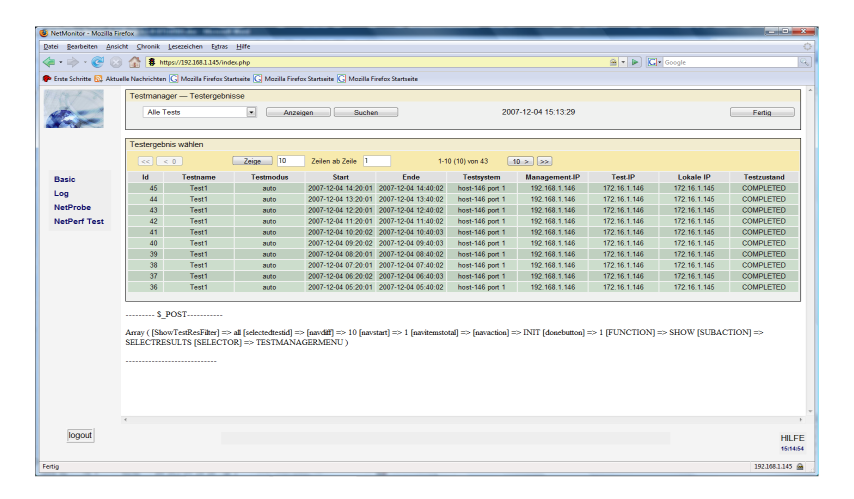


Abbildung 85: Testergebnisse

Wie in Abbildung 85 zu erkennen, werden die einzelnen Testergebnisse, mit fortlaufender Nummer angezeigt. In den dahinter liegenden Spalten, sind die Eck Daten des Tests zu sehen, die sich wie folgt beschreiben.

- Test ID = fortlaufende Nummer, der Tests
- Test Name = Name des Tests, den man in der Test Definition vergeben hat
- Test Modus = Ob der Test, in der Definition auf auto oder manuell gestellt worden ist
- Start = Wann der Test gestartet worden ist
- End = Wann der Test beendet worden ist
- Test System = von welchem System und von welchem Port aus der Test durchgelaufen ist
- Management IP = Die Management IP des Remote Systems
- Test IP = Die Test IP des Remote Systems
- Lokale IP = Die IP Adresse des Testsystems
- Test Zustand = Ob der Test erfolgreich durchgelaufen ist, oder ob er mit einem Fehler beendet worden ist

Um sich die genauen Daten eines Tests anzeigen zu lassen, braucht der zutreffende Test nur angeklickt werden. Sind die Daten am Bildschirm sichtbar, kann man sich zum einem, das Testlog anzeigen lassen und zum anderen, sich den Test Grafisch Darstellen lassen. Beides ist in Abbilddung 86 und 87 ersichtlich.

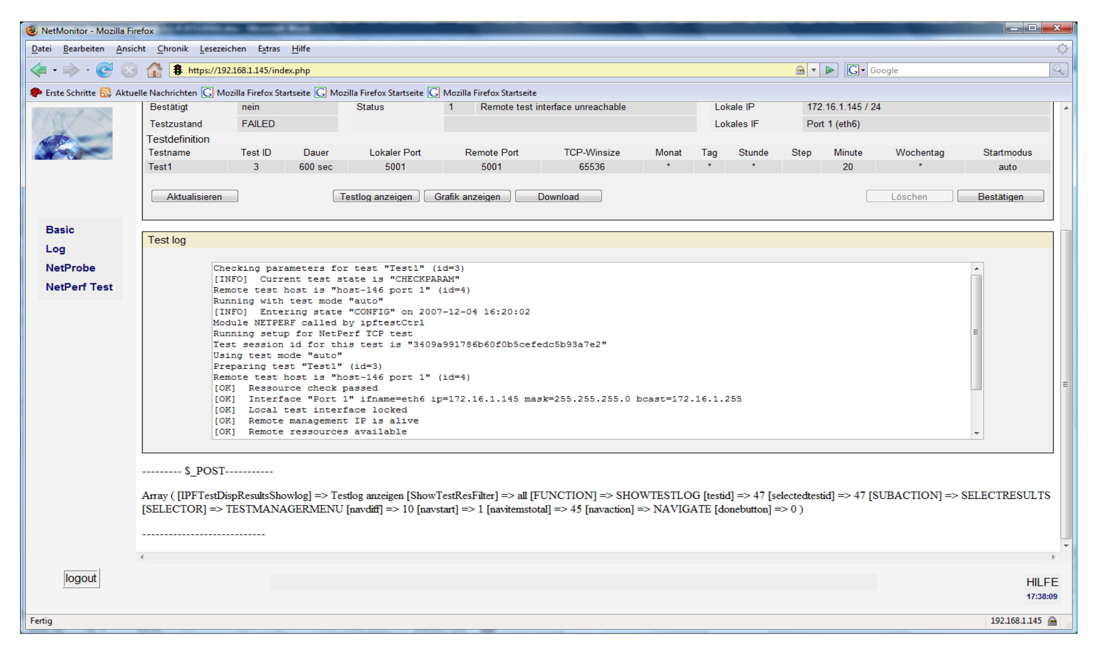


Abbildung 86: Testlog des durchgeführten Tests

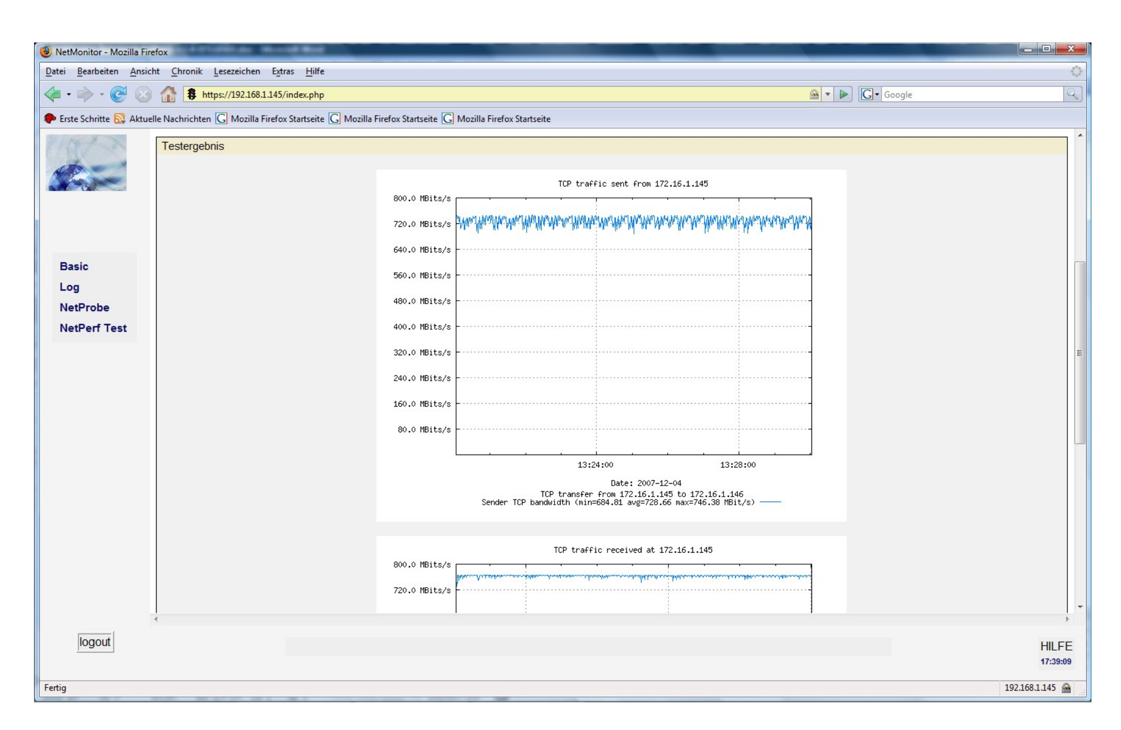


Abbildung 86: Grafisch Darstellung des Tests

Nun, kann auch der durchgeführte Tests, über den Button Download, auf der Lokalen Festplatte aubgespeichert werden. Wenn der Button, betätigt wird, erhält man folgende Foglichkeiten.

Downlod:

- Diagramm (local → remote) = Grafisch Darstellung, des Test vom Localem zum Remote Systems
- Diagramm (remote → local) = Grafisch Darstellung, des Test vom Remote zum Localem Systems
- Testparameter (CSV) = eine auf Text basierende Datei, wo die Testparamenter dargestellt werden

Dies auswahl wird getroffen, indem die Makierung, im davor liegendem Kasten gesetzt wird. Wichttig hierbei ist es noch zu beachten, das nur eine auswahl getroffen werden kann. Weden mehrere Darstellungen des Tests benötigt, müssen die aufgeführten Schritte, erneut durchgeführt werden.

9.6 Test Definition ändern

Um einen betsehenden Test zu ändern, geht man wie folgt vor. Auf der Startseite von Iperf Test, wird als erstes das Testsystem ausgewählt und anschließend mit dem Button Testdefinieren bestätigt. Ist die neue Seite geladen, bekommt man wie zuvor bei der Testdefinition, die Maske wo ein neuer Test erstellt werden kann. Hierbei kann aber auch anstatt auf die Schrift auf den, dem Testsytem zugeordneten Tests geklickt werden und somit die werte det Testeinstellungen geändert werden, wie in der folgenden Abbildung zu sehen ist.

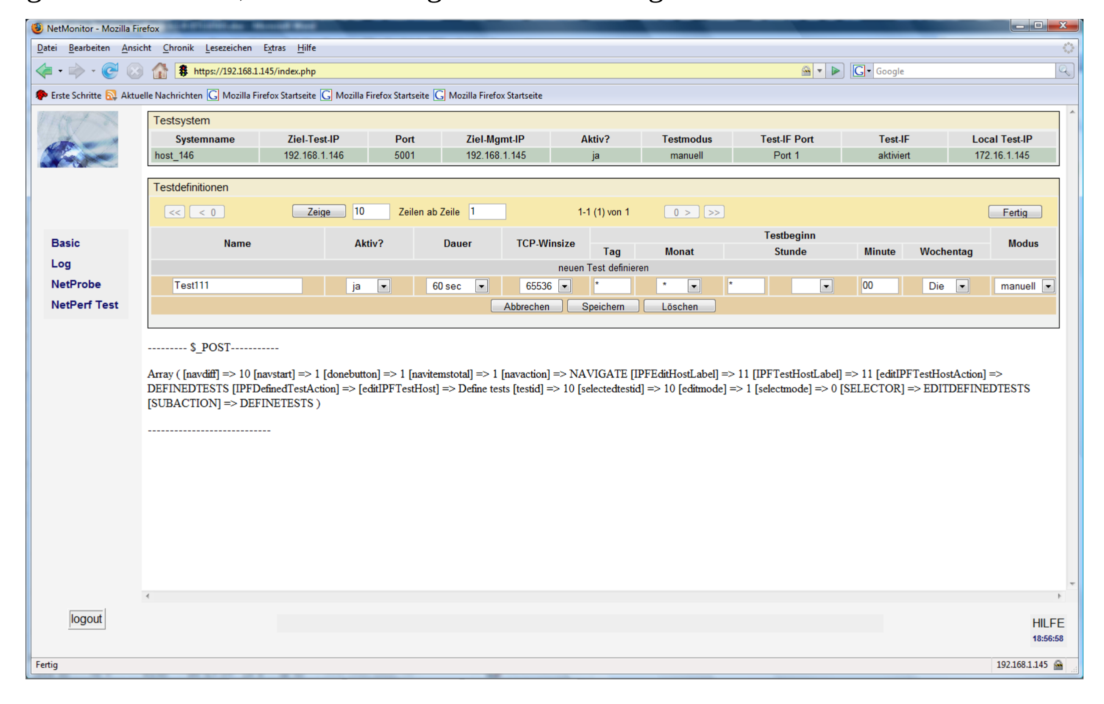


Abbildung 87: Bestehende Testeinstellungen ändern

Sind die Einstellungen geändert worden, brauch die Test definition nur über den Button Speicher und anschließend über Fetig bestätigt werden und somit gelangt man zu ausgangs Bildschirm zurück.

9.7 Testergebnisse löschen

Um einen durchgeführten Test zu löschen, muss auf der Startseite von Iperf Test, wider das Testsystem von wo aus der Test durgeführt worden ist, ausgewählt werden. Hat man dieses gemacht, wird dieses mit dem Button Test definieren, bestätigt. Nun gelangt man wider, zur eingabe Maske wo ein Test definiert oder geändert werden kann. Hier wir der Test ausgewählt den man Löschen will, die geschieht durch einfaches anklicken. Ist diese geschen, werden wie in der nachfolgenden Abbildung zu sehen, die Button Abbrechen, Speichern und Löschen Aktiv.

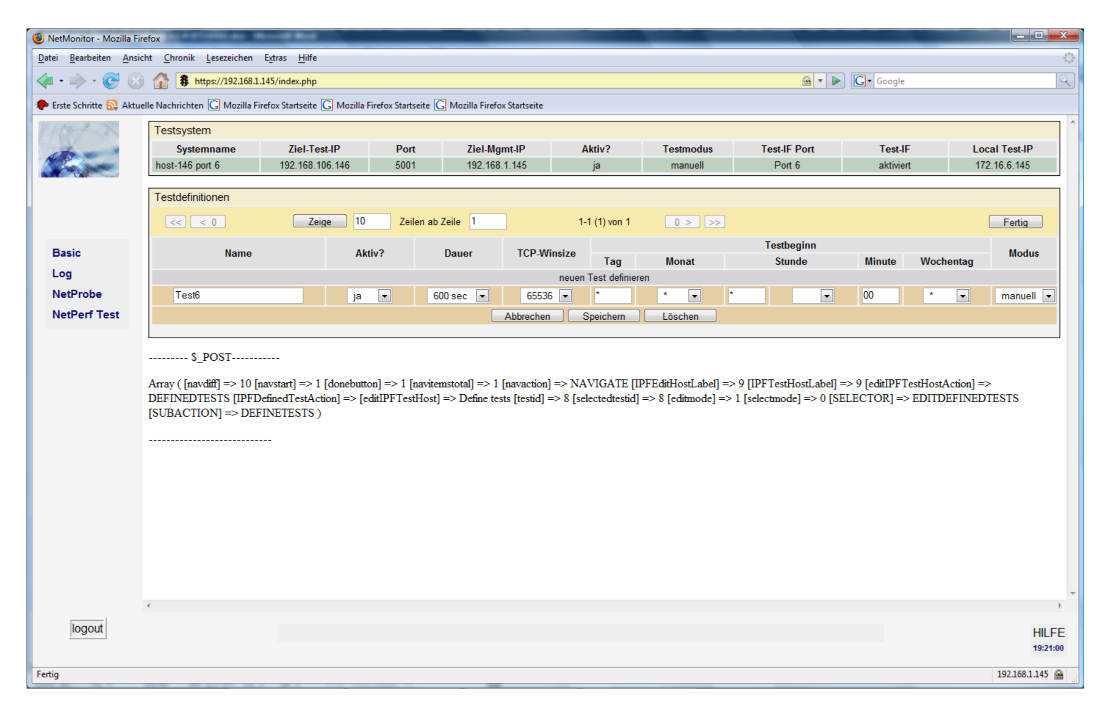


Abbildung 88: Löschen eines Tests 1

Um den Test zu Löschen, wird die Seite mit dem Button Löschen bestätigt. Die nun, wie in der nächsten Abbildung zu sehenden Meldung, wird mit OK bestätigt.

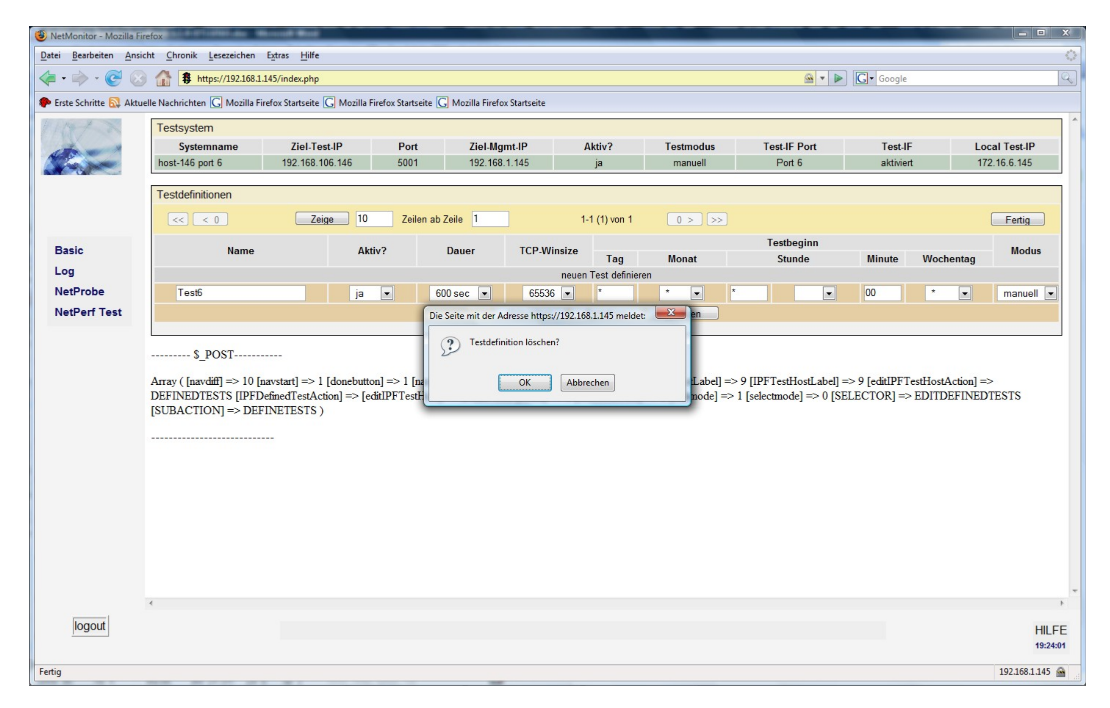


Abbildung 89: Löschen eines Tests 2

Ist die Meldung, mit OK bestätigt worden, bekommt man zu Abschluß noch die Meldung, das der Test erfogreich gelöscht worden ist.

9.8 Laufende Tests Abbrechen

Um einen Laufenden Test Abzubrechen, geht man auf der Startseite im oberen Bereich unter Testmanager auf Test Abbrechen. Im nachfolgendem Fenster, werden dann alle Tests angezeigt die Momentan am Laufen sind. Hierbei klickt am den Laufenden Test, den man Abbrechen möchte an und gelangt somit auf folgende Seite.

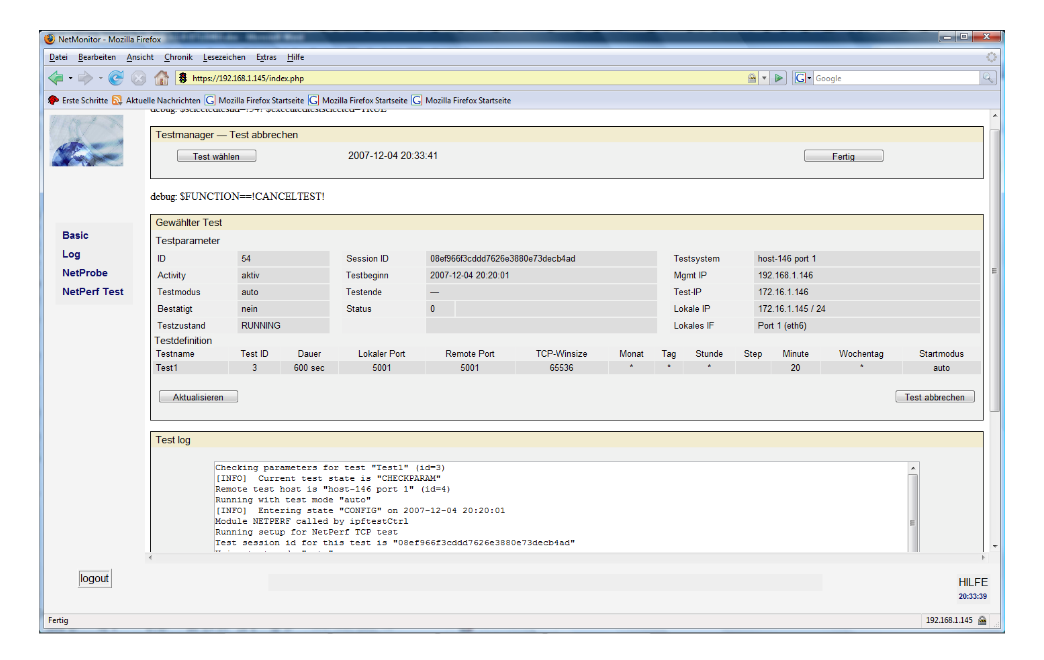


Abbildung 89: Test Abbrechen

Zum Abschluß, brauch nur noch auf den Button Test abbrechen geklickt werden und bei der nachfolgenden Meldung auf OK, damit der Test vorzeitig Beendet wird.

10 Erstellen eines TCP Tests

Um einen TCP Stream Test, von einem Localen System zum Remote System zu erstellen, geht man wie folgt vor.

Als erstes beginnt man mit der Kofiguration des Localen Systems. Hierzu muss man sich erst man System angemeldet werden, dazu muss ein Internet Browser geöffnet werden, wo in der Adress Zeile, die IP des Lokalen Systems eingetragen wierd, in userm Beispiel, sieht es so aus.

https://192.168.1.145

Die nachvolgenden Zertifikats aufvorderungen, müssen mit ja Beantwortet werden. Im nächsten schritt wird sich mit Benutzer Namen und Passwort am System angemeldet.

Somit erhält man eine Browser Seite, wo an der Linken Seite einigi Menü Punkte stehen, hier wird der Menü Punkt Netperf Test ausgewählt.

Im ersten Schritt wird das Lokale Test Interface Kofiguriert, hierzu klieckt man, auf der Startseite von Netperf Test auf den Button Lokale Einstellungen/Einstellungen. Nun erscheint ene neue Seite, wo zunächst unter Test Interface Konfigurieren, im ersten Pull Down Menü der Port ausgewählt, im zweiten Pull Down Menü, sollte hier aktiviert ausgewählt werden und in den nachfolgenden Feld muss die IP Adresse die für das Lokale System bzw. dem Port vergeben werden soll. Im lesten Feld muss die Subnetz Maske eingetragen werden, allerdings in Bits.Sind die Einstellungen alle vorgenommen worden, brauch nur noch mit Speicher die Kofiguration abgespeichert werden.
Ganz wichtig ist es, diesen Schritt zu Kofigurieren des Interfaces, auch auf dem Remote System vorzunehmen. Dazu, muss man sich am Remote System, genauso wie oben beschrieben Anmelden und das Lokale Test Interface Konfigurieren. Alle weiteren Einstellungen, die ab jetzt beschrieben werden, brauchen nur am Localen Test System vorgenommen wedern.

Nun begebenn wir uns wieder am Localen System, auf die Startseite von Netperf Test und erstellen im nächsten Schritt, ein Testhost. Hierzu, klieckt man im mittleren Bereich unter Testsysteme auf Neu. Im nunfolgenden Fenster werden fogende Einstellungen gemacht.

- Name = ein beliebiger Name für den Test Host
- Remote IP = Ip – Adresse, des Remote Systems
- Management IP = Management Ip – Adresse, des Remote Systems
- Testmodus = Ob der Test Automatisch oder Manuell durchgeführt werden soll
- Lokales Test IF = auf welchen Port das Lokale Test Interface liegt

- Verwenden = ob der Test Host sofort Verwendet werden soll, oder später

Sind diese Schritte durchgeführt worden, bestätigt man die Einstellungen mit Neu und der Testhost erscheint im unteren Bereich der Seite.

Im nun folgendem Schritt, wird ein Test definiert, hierzu geht man wieder zur ausgangs Seite von Netperf Test und im mittleren Bereich, wird zunächst unter Test Systeme im Drop Down Feld, das Test System ausgewählt und anschließend auf den Button Test definieren geklickt. Anschließend, gelangt man zu einer Neuen Seite, wo im oberen Bereich das Test System steht und im unteren Bereich, die Test Definitionen. Hierzu muss allerdings erst eine Definition erstellt werden. Hierzu wird auf die Schrift neuen Test definieren geklickt. Im Anschluss, werden die nachfolgenden Felder ergenst. Dieses geschieht wie folgt.

- Name = beliebiger, aber eindeutiger Name, des Test´s
- Aktiv = ob der Test Aktiviert werden soll oder noch nicht
- Dauer = Hier kann die Dauer der Zeit eingestellt werden, wie lange der Test, in einer Richtung laufen soll. Zur Info, wenn z.B 180 eingestellt wird, benötigt der Test 2 x 180 Sekunden, da der TCP Stream in beiden Richtungen erfolgt.
- TCP-Winsize = unter diesem Punkt, kann der TCP Stream eingestellt werden
- Tag = an welchem Tag, der Test laufen soll, bei Stern Täglich
- Monat = in welchem Monat der Test laufen soll, bei Stern Monatlich
- Stunde/Minute = zur welcher Uhrzeit der Test laufen soll, bei Stunde kann ein Stern für Stündlich eingesetzt werden, bei Minute muss eine Zahl eingetragen werden.
- Wochentag = an welchem Wochentag der Test laufen soll, bei Stern Wöchentlich.
- Modus = ob der Test manuell oder automatisch gestartet werden soll. Wobei, wenn hier automatisch eingestellt wird, darauf zu achten ist, das in der Konfiguration des Test Interfaces, auch automatisch stehen muss.

Sind alle Felder ausgefüllt, brauch der Schritt nur noch mit Speicher bestätigt werden.

Nun sind alle Einstellungen getroffen, damit ein TCP Stream Test laufen kann. Je nachdem, was für Werte man bei der Test Definition eingestellt hat, sollte der Test zu der angegebenen Zeit beginnen. Der Test kann aber, zu jeder Zeit über die Startseite von Netperf Test im oberen Bereich, anhand des Buttons Manueller Test, manuell gestartet werden.